MARCH 2019

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Competence Center Europe – Smart Buildings

Thorsten Reibel, Jürgen Schilder, Stefan Grosse, Martin Wichary & Ilija Zivadinovic

 Document ID.: Rev.:

Agenda

Overview IP Router

Situation and Threat scenarios

KNX Secure (KNX IP Secure and KNX Data Secure)

IP Router Secure IPR/S 3.5.1

Commissioning of IP Router Secure

Attacks over the IP network

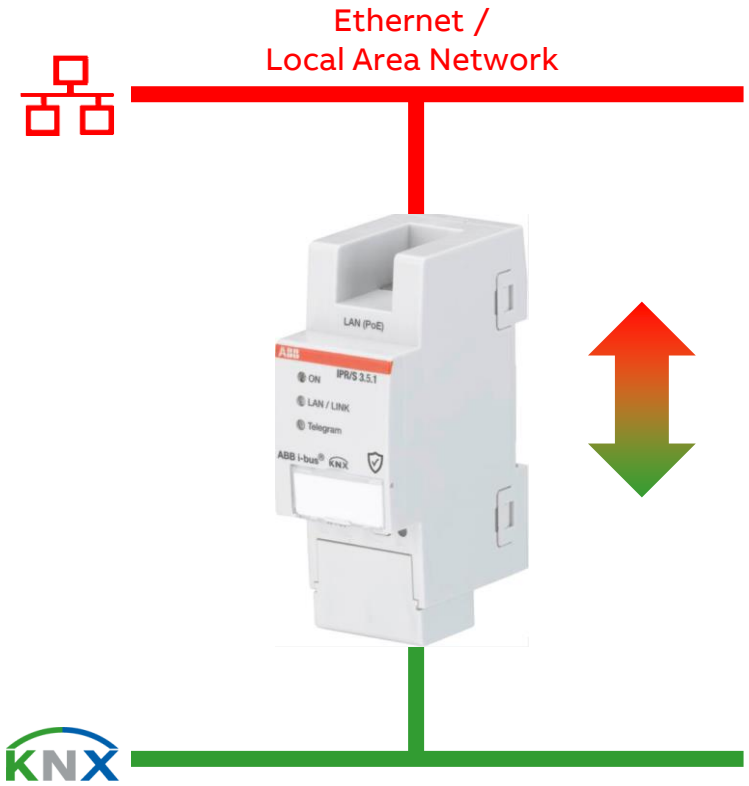
ABB i-bus® Tool

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

IP Router

Principle

- An IP Router converts KNX (TP) telegrams into IP network telegrams (KNXnet/IP) and vice versa
- This allows data exchange between KNX and IP networks
- The IP Router can be used as a line or area coupler and complies with the specifications of the KNXnet/IP standard
- Together with the ETS, the IP Router can program devices via LAN



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

KNXnet/IP Capabilities

Routing (Coupler)

– Connection of KNX Lines and Areas over IP

– Routing of KNX telegrams

Tunneling (Interface)

– To connect a PC to KNX via IP

- ABB i-busTool
- Working with ETS (download, diagnostics,…)
- Visualisation
- Connection of Tablet/Smart Phone with App via Wi-Fi

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

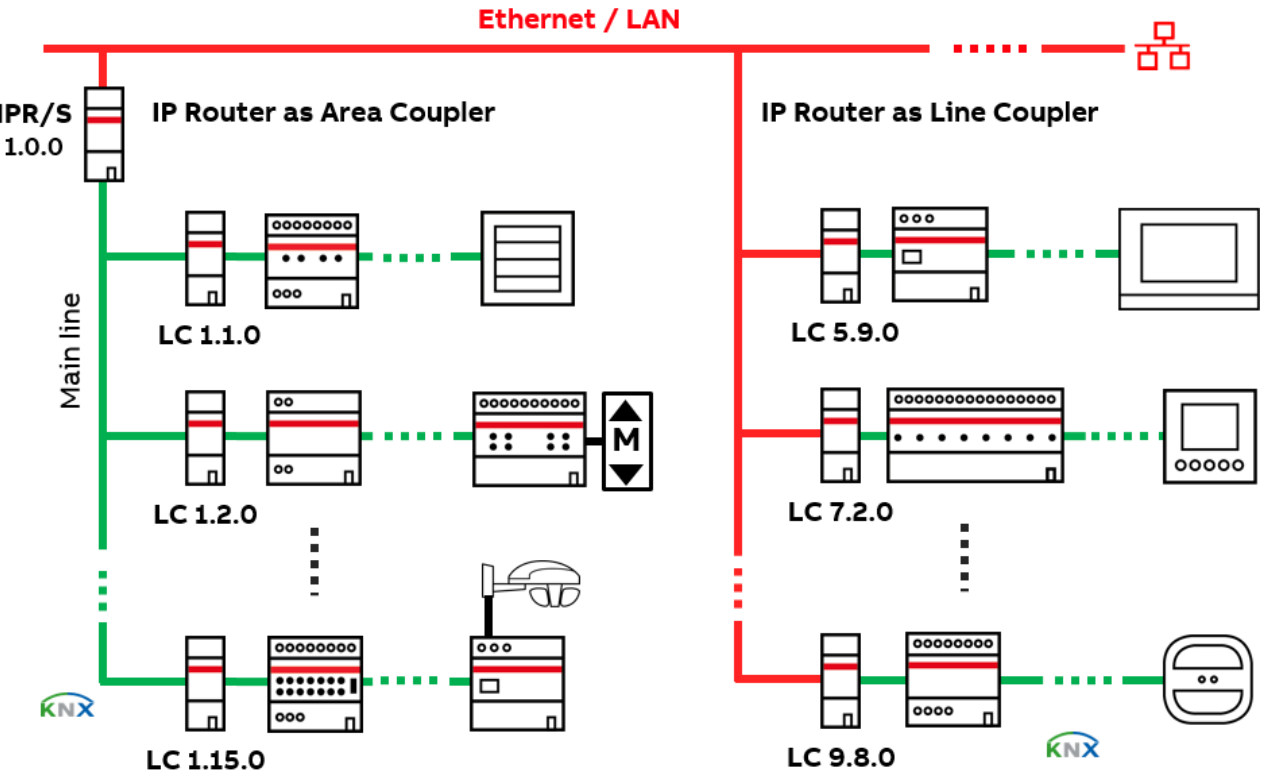
KNX telegrams in the network – Multicast

- Multicast designates communication of a transmitter with a group of receivers
- The IP Router Secure sends the KNX telegrams packaged as UDP/IP telegrams on the IP network, and all IP Router Secure devices parameterized with the same multicast address receive and evaluate these telegrams
- If a telegram is intended for the corresponding subline, the IP Router Secure routes the telegram into the line – otherwise, it is rejected
- The IP Router Secure sends telegrams from the KNX to the IP network in accordance with the KNXnet/IP protocol specification
- This multicast IP address 224.0.23.12 port 3671 is the defined address for the KNXnet/IP from the KNX Association in conjunction with IANA for KNX IP devices
- In order for several IP Router Secure devices to communicate with one another in a network, multicast communication must be possible between the devices (e.g. routers, switches or firewalls)

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

IP Router: Routing – Coupler

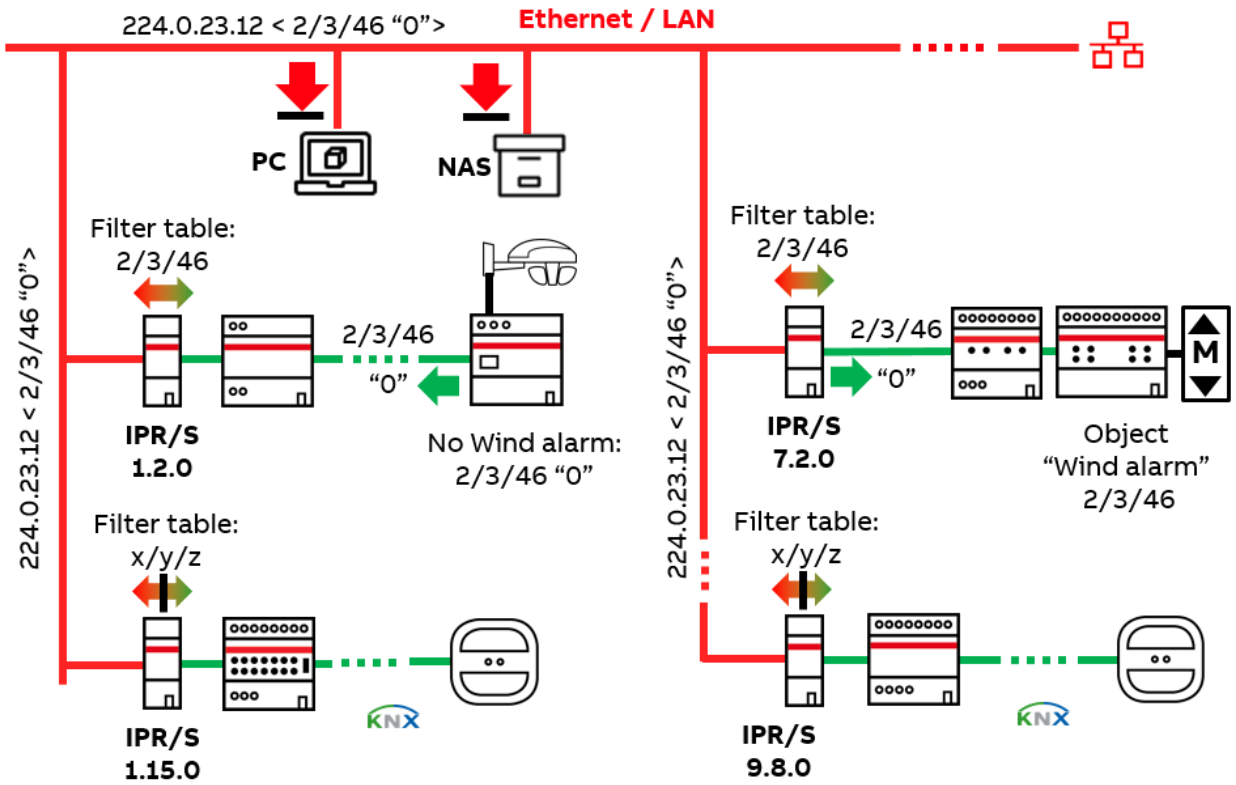
Connection “KNXnet/IP Routing“: Multicast (Point to Multipoint)



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

IP Router: Routing – Coupler

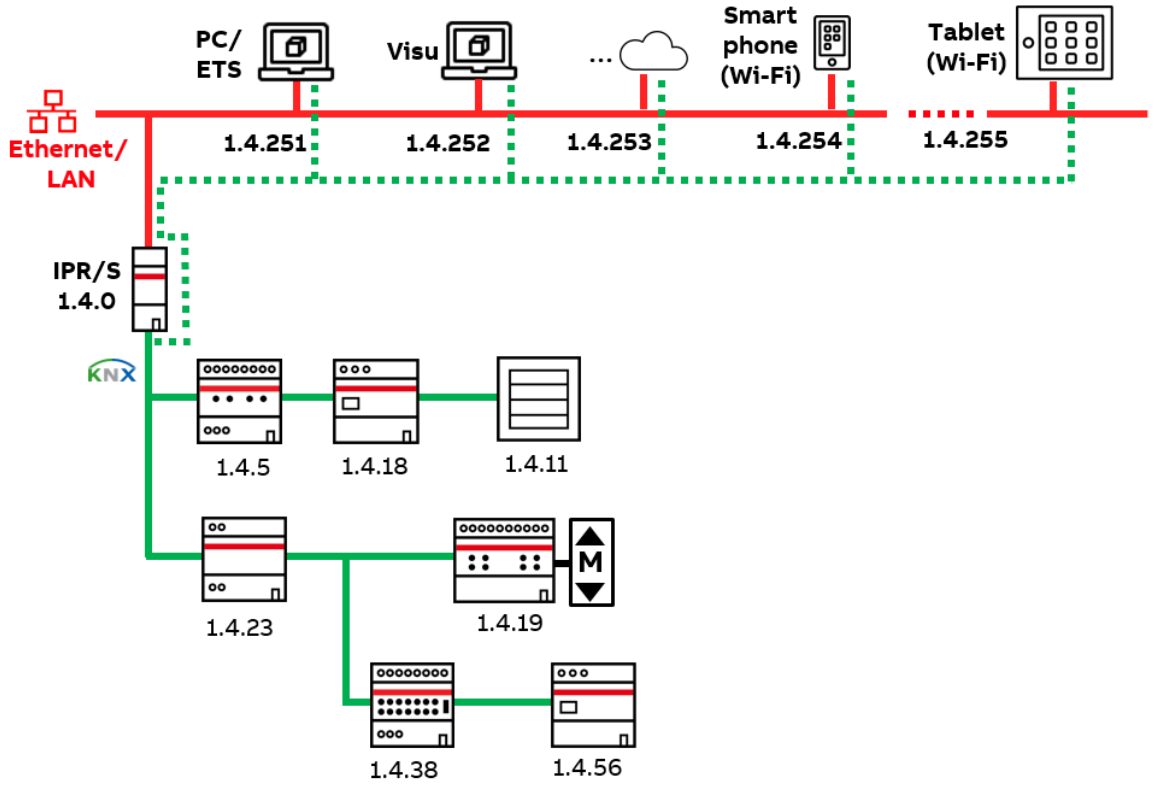
Connection “KNXnet/IP Routing“: Multicast (Point to Multipoint)



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

IP Router: Tunneling – Interface

Connection “KNXnet/IP Tunneling“:
Unicast (Point to Point)
ETS: Group and bus monitor
1.4.0 Individual address IP Router
Tunneling Server e.g. 1.4.251 – 1.4.255:
→ 5 additional addresses (local) for the tunneling server of the IP Router



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

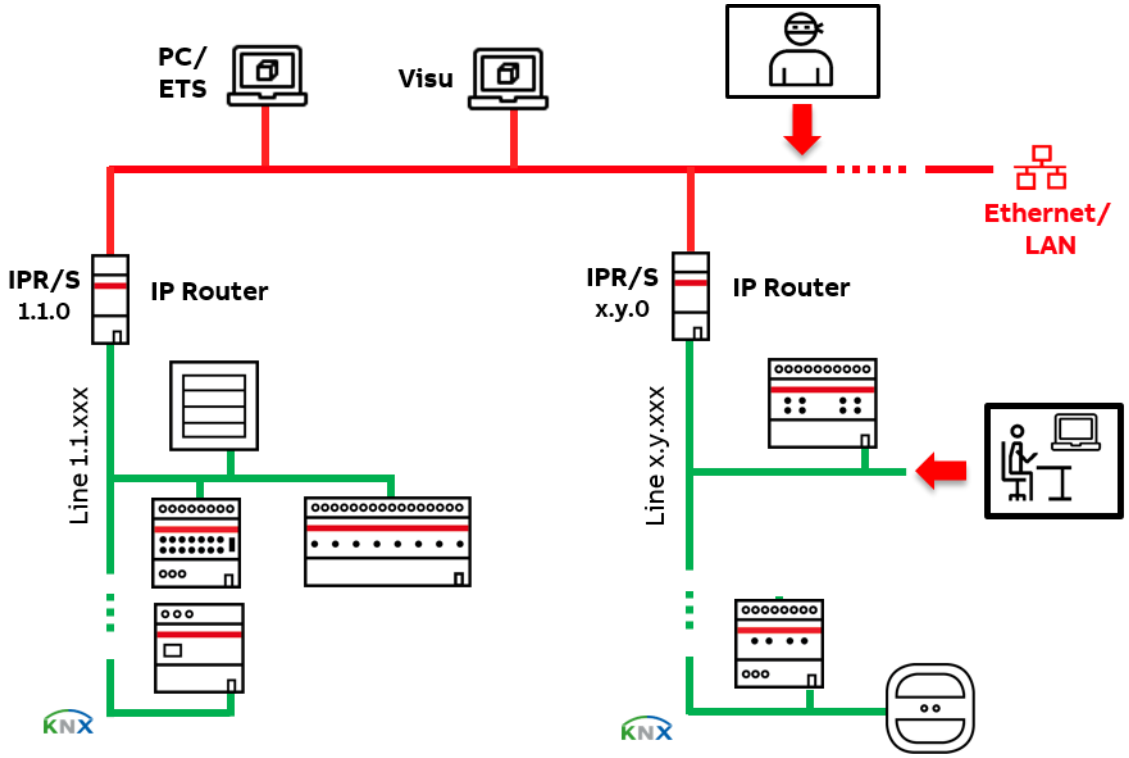
Bus safety from the perspective of a manufacturer

- Residential and functional buildings have been equipped with intelligent bus technology for 25 years
- Increasing opening towards the Internet and smart devices
- This increases comfort, safety and efficiency, but also the risk of attacks on the building infrastructure
- Buildings cannot be made absolutely secure, but the effort of an attack can be increased and the impact limited locally
- There are technical, organizational and planning aspects to consider

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Situation

- The most relevant attack scenario on a KNX installation is over the IP network
- But access over TP is of course also possible and relevant for Building Automation



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Threat scenarios

IP network

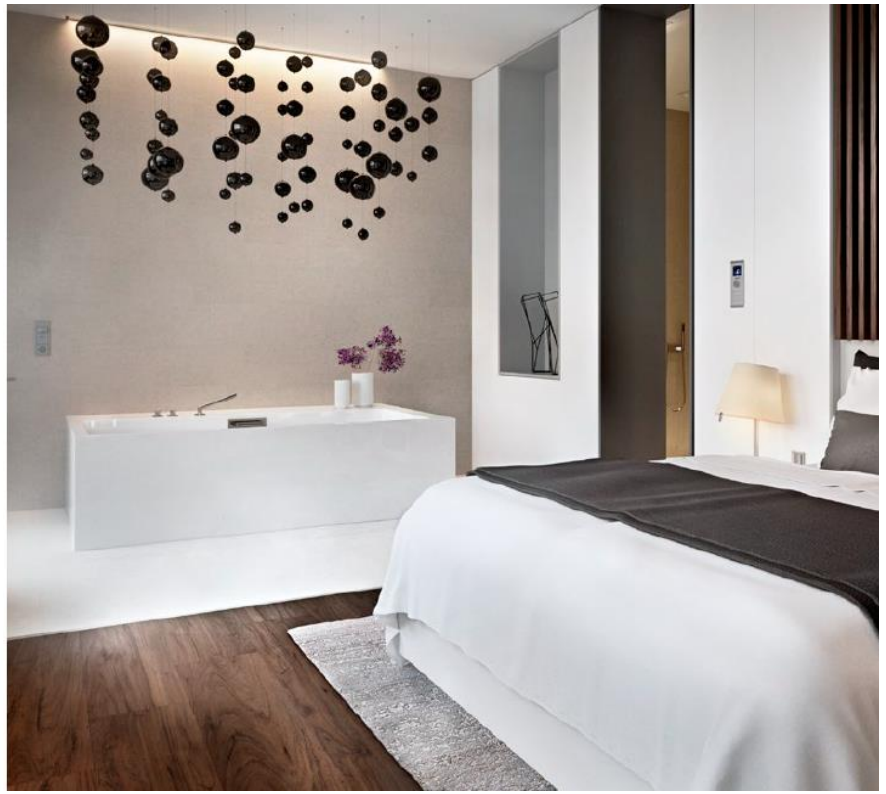
– Local (Wi-Fi/LAN)
  - Often no separate technical network; therefore, users have direct access to IP communication

– Remote access / Internet:
  - Network Routers are often "open" visible on the Internet
  - High number of potential attackers

Fieldbus

– Private housing
  - KNX cable outside the building

– Commercial buildings
  - Access to the bus via any node (especially in the hotel)



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Attack types (examples)

Denial of Service Attack (DOS)

– Telegram flood on KNX (IP) device, as a result the device is temporarily unavailable

Doing unwanted functions

– Driving blinds, switching lights, …

Sabotage

– Change set points, reprogram devices, short circuit bus

Espionage

– Spying on user profiles

Deceive, intrusion

– Opening a door, disabling/unset security systems

Impacts

Possible impacts

– Image damage (manufacturer, system integrator, end customer)

– Data loss

– Reduction of comfort

– Security loss

– Economic damage

→ There are already ways to prevent / significantly hinder access to the system

→ Due to the current enhancements of the KNX standard ("KNX Secure"), additional security mechanisms are possible

→ KNX Secure alone does not make the system secure!

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

The “entire chain” must be taken into account

Manufacturer

- (Product) security standards (cyber security, robustness), updates
- Specification of standards (KNX Secure)
- Provision of checklists, training, …

System integrator, installer

- Safety concept for planning, installation and operation
- Risk analysis

End customer, operator of the building

- Access control, security concept
- IT security (current security settings ...)

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

General measures

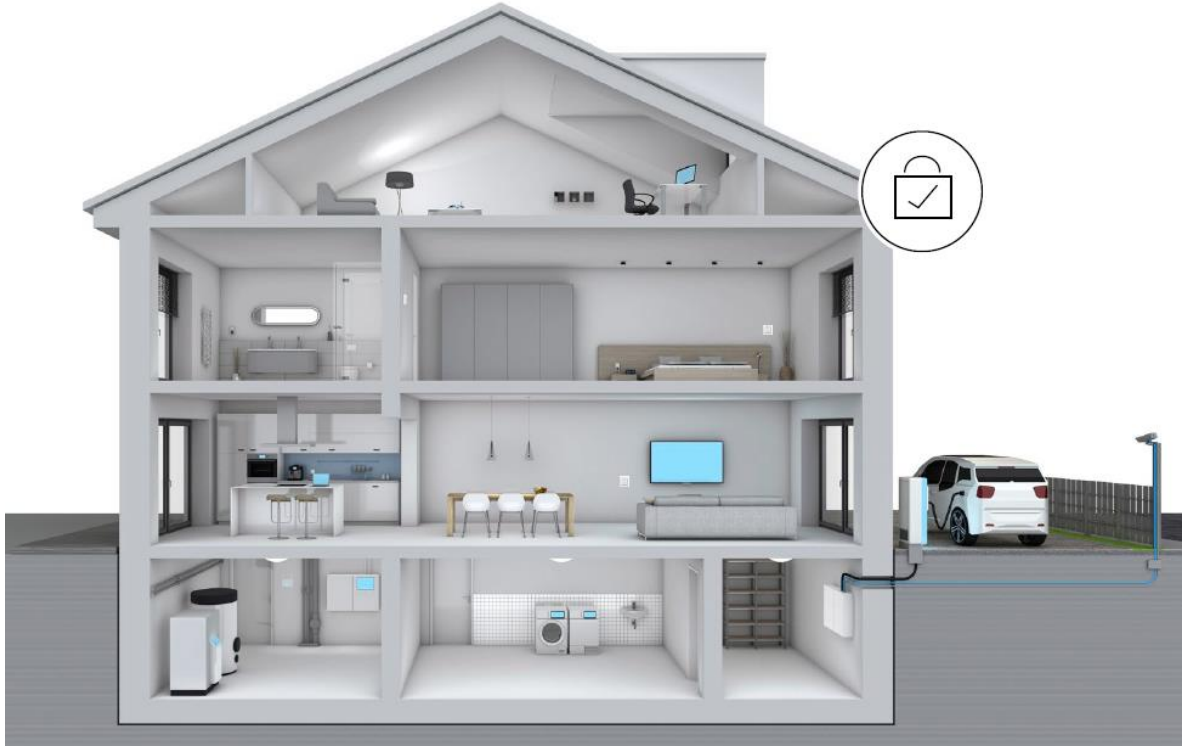
Cybersecurity must be an integral part of planning and execution a facility

Already it is possible to make access via IP (relatively) secure

- To the outside (firewall, VPN, filtering MAC addresses)
- Inside (separate technical IP network, encryption with Wi-Fi)

Prevent physical access to the bus

- Lockable distribution boards
- Devices with dismantling protection
- Separate lines for sensitive areas
- No KNX cable outside the building
- …



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Special solution for the attack scenario from the field level

Standard IP Interfaces connect hotel rooms with a central system (BMS Server)

Tunneling connection from each room to central BMS

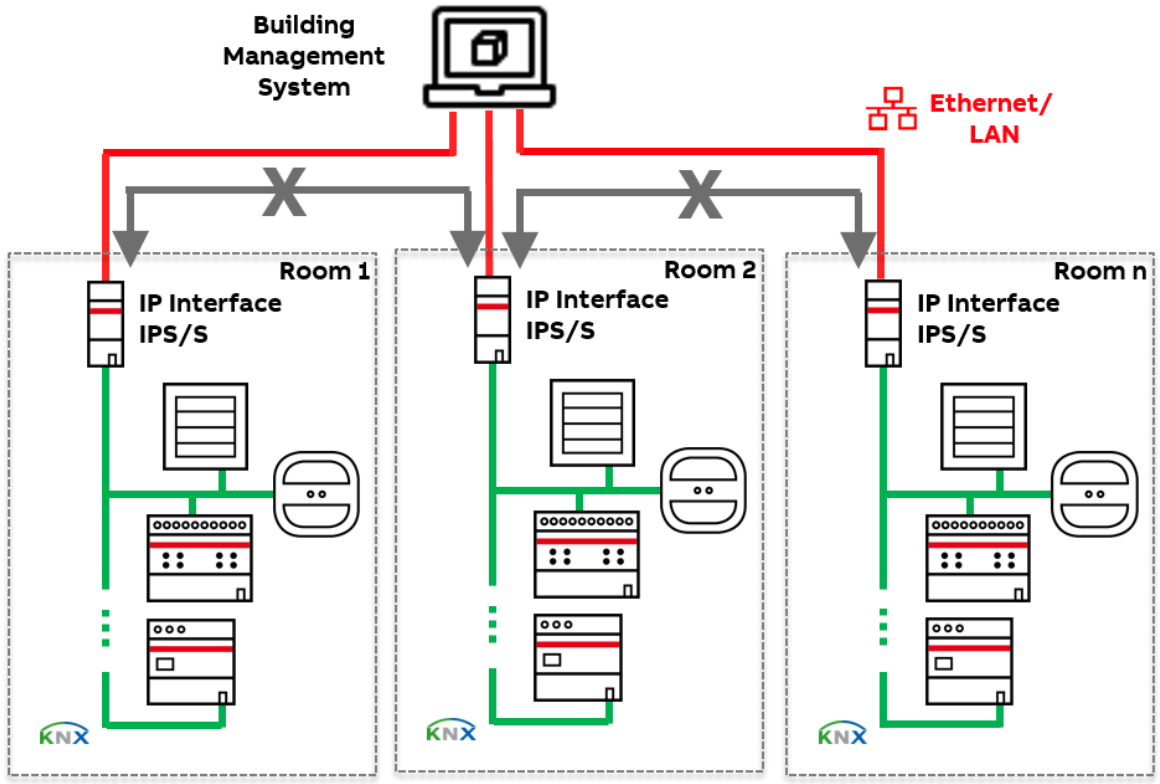
Security by isolated rooms – no KNX Secure!

It covers the use case „Attack” from the field level

No direct inter-room communication available

BMS can also monitor the KNX field devices

→ ABB “Hotel IP Link Bundle” HIL/S 20.1.1

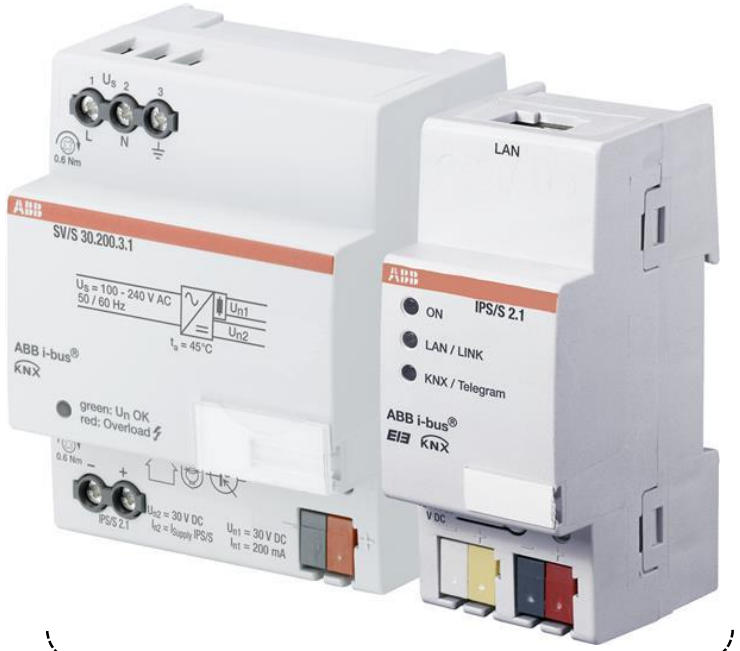


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Special solution for the attack scenario from the field level

ABB “Hotel IP Link Bundle” HIL/S 20.1.1

- The Hotel IP Link Bundle is consisting of a KNX IP Interface (IPS/S) and a KNX Power Supply (SV/S)
- The IPS/S supports the KNXnet/IP protocol (tunneling) from the KNX Association
- A central system (BMS server, visualization system, hotel management system) establishes a connection to each individual IP Interface IPS/S via the integrated tunneling server
- The SV/S generates and monitors the KNX system voltage for up to 20 KNX TP (twisted pair) devices via an integrated choke
- The additional 30 V DC voltage output is used to power the IPS/S 2.1
- Order no.: 2CDG110237R0011



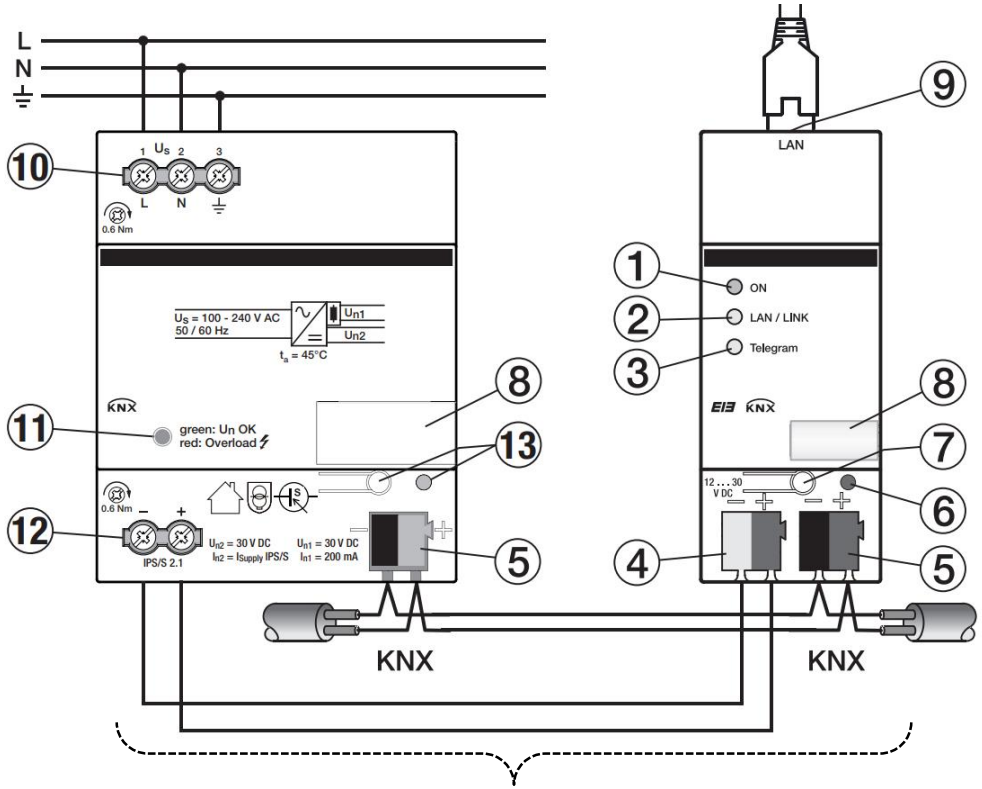
IP Link Bundle HIL/S 20.1.1

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Special solution for the attack scenario from the field level

ABB “Hotel IP Link Bundle” HIL/S 20.1.1

1. ON LED
2. LAN/LINK LED
3. Telegram LED
4. Supply voltage connection
5. Bus connection terminal
6. Programming LED
7. Programming button
8. Label carrier
9. LAN connection
10. Power supply connection Us
11. Status LED
12. IPS/S 2.1 connection



IP Link Bundle HIL/S 20.1.1

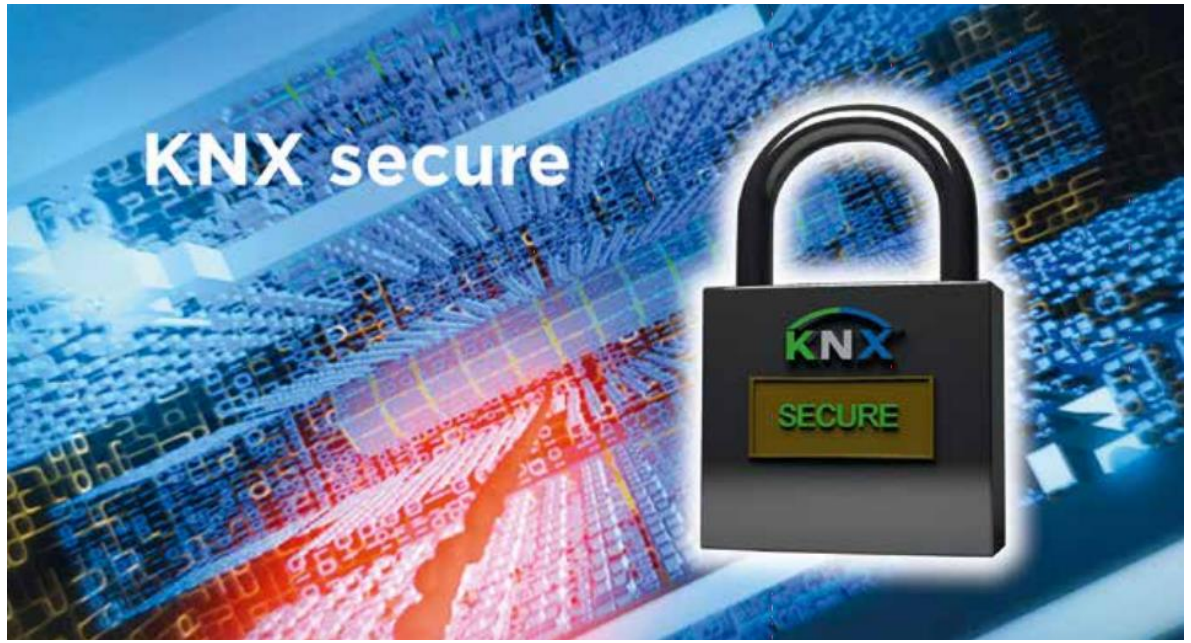
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Measure KNX Secure

KNX Secure has been developed to respond to the current and future challenges regarding cyber security in building automation

– Step 1: Securing the IP communication with "KNX IP Secure"
  - Implementation of the KNX IP Secure Standard in routers, interfaces and other IP devices
  - Software clients (visualizations) are also affected

– Step 2: Implementation of “KNX Data Secure” in all field devices



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

KNX Secure offers maximum protection

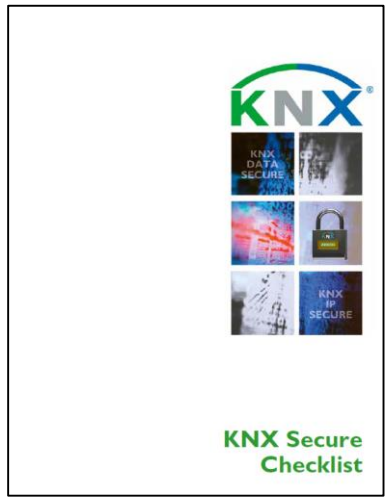
- Home and building automation with KNX is secure
- KNX Secure guarantees maximum protection
  - KNX IP Secure extends the IP protocol in such a way that all transferred telegrams and data are completely encrypted
  - KNX Data Secure effectively protects user data against unauthorized access and manipulation
- The KNX technology is standardized according to EN 50090-4-3, which means that KNX successfully blocks hacker attacks on the digital infrastructure of networked buildings
- Thus minimizing the risk of digital break-ins
- Moreover, KNX Secure meets the highest encryption standards (according to ISO 18033-3, such as AES 128 CCM encryption) in order to effectively prevent attacks on the digital infrastructure of buildings and to achieve the highest level of data protection

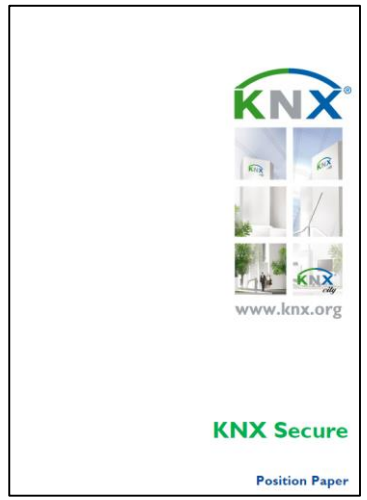
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

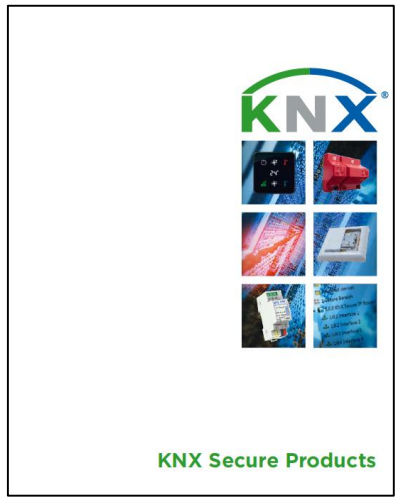
KNX Secure Brochures of the KNX Association

- KNX Secure Checklist
- KNX Secure Position Paper
- KNX Secure Products

- https://knxsecure.knx.org







Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Conclusion

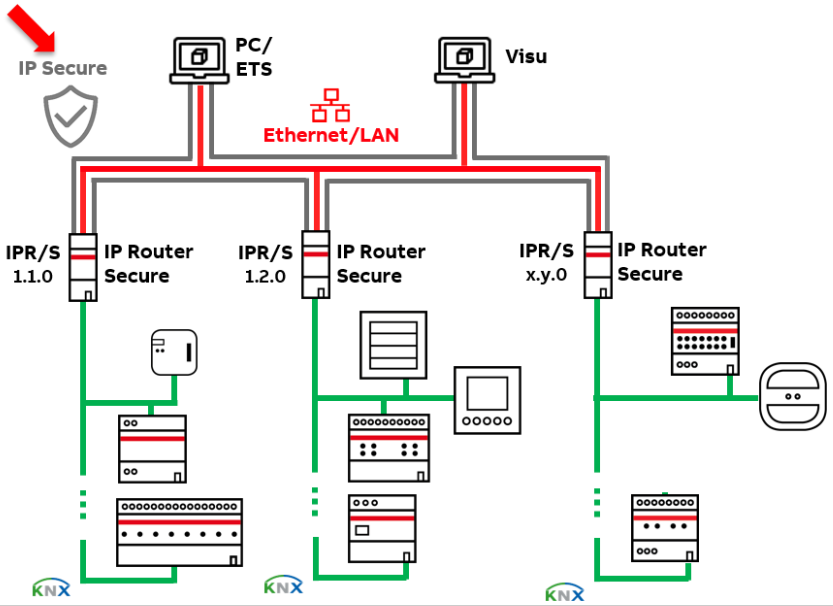
- There is no 100% security
- Manufacturers, KNX Association, associations and the system integrators are pushing the issue of safety to make the building (even) safer
- Safety, comfort and economy have to be balanced against each other
- In each project, it must be weighted how much security is necessary
- The entire lifecycle of a building must be taken into account
- Integrators with the appropriate know-how have a competitive advantage and should use it

Elbphilharmonie (Hamburg)
Concert hall/Stadiums and recreation

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

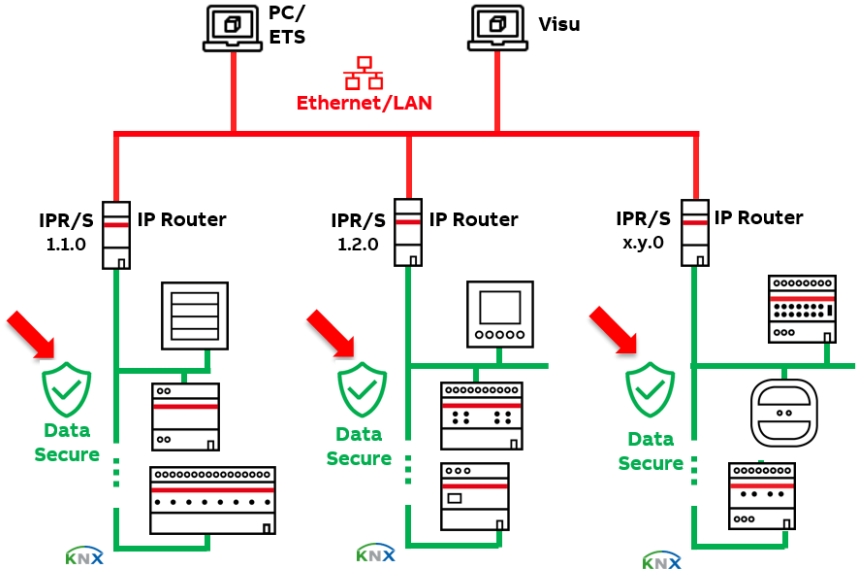
KNX IP Secure (KNXnet/IP Secure Routing and Tunneling)

- TP Telegrams are wrapped in a secure frame on IP
- Tunneling connections are secure
- All IP devices in a project have to speak secure



KNX Data Secure

- Each individual group telegram can be encrypted
- Data Secure means effort; every field device has to be changed (hardware and software)



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1

The ABB IP Router Secure is a KNX device according to the KNX Secure Standard (KNXnet/IP Security)

- The communication on the IP backbone is secure (multicast communication)
  → All KNX IP devices must support the KNXnet/IP security protocol
- ETS5 and the current version of the device application are required for programming
- The device can be safely put into operation
- All tunneling connections are encrypted
- Firmware Update with ETS App, available in KNX Online Shop

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Summary of the features

The IP Router Secure has the same properties (ETS parameter, filter table, …) as the standard IP Router IPR/S 3.1.1

- 5 Tunneling Servers → parallel access, less hardware
- Power over Ethernet (PoE) → no additional power supply or 12…30 V DC
- ABB i-bus Tool support → easier commissioning and diagnostic
- Smart housing concept → better and safer installation, wiring and commissioning
- Unicast Communication → Solution if Multicast is not possible
- Network management function “Monitoring for KNX bus voltage failure“ → improved performance of the complete solution
- Support of full filter table for all main groups 0…31 → no restrictions for usage of the extended group address range

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

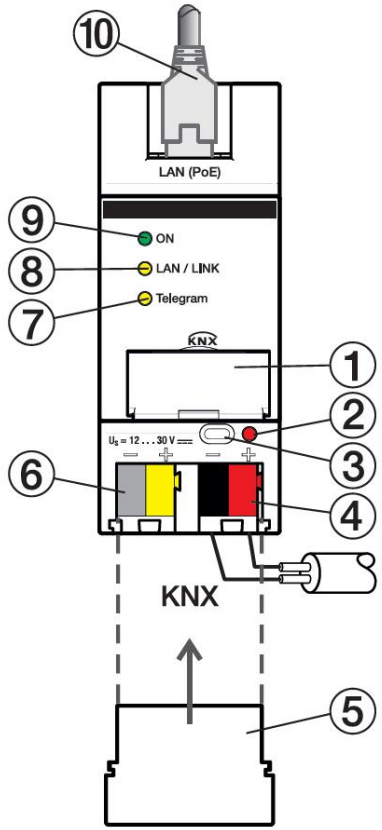
ABB IP Router Secure IPR/S 3.5.1 – Technical Data

- Housing and form factor similar to IPR/S3.1.1
- 2 MW standard DIN rail component
- Supply voltage Us 12...30 V DC (+10% / -15%)
  and/or
- PoE (IEEE 802.3 af class 1)
- LAN connection 10/100 BaseT, IEEE 802.3 via RJ45 plug
- Power loss Max. 1.8 W
- Current consumption
  - Supply voltage Us Max. 120 mA at 12 V
  - KNX < 10 mA

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Device connection

1. Label carrier
2. KNX programming LED (red)
3. KNX programming button
4. KNX bus connection terminal
5. Cover cap
6. Power supply connection Us
7. Telegram LED (yellow)
8. LAN/LINK LED (yellow)
9. ON LED (green)
10. LAN connection



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Operation and display

ON

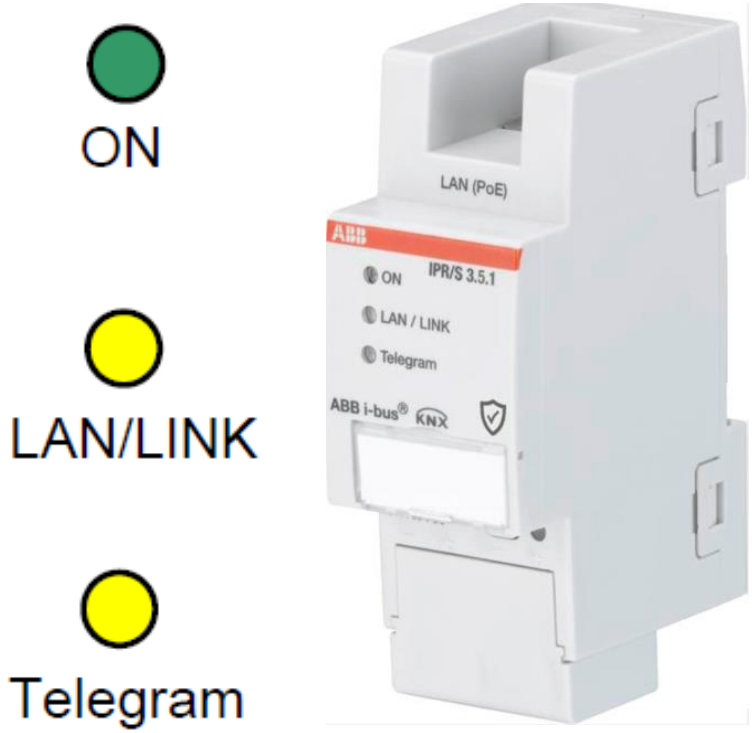
- After the supply voltage Us is connected, the LED initially lights up continuously
- After approx. 40 sec., the LED starts flashing until initialization is complete

LAN/LINK

- Once initialization is complete, the LED lights up when the supply voltage Us is present and the Router is connected to an IP network
- The LED flashes with data traffic on IP

Telegram

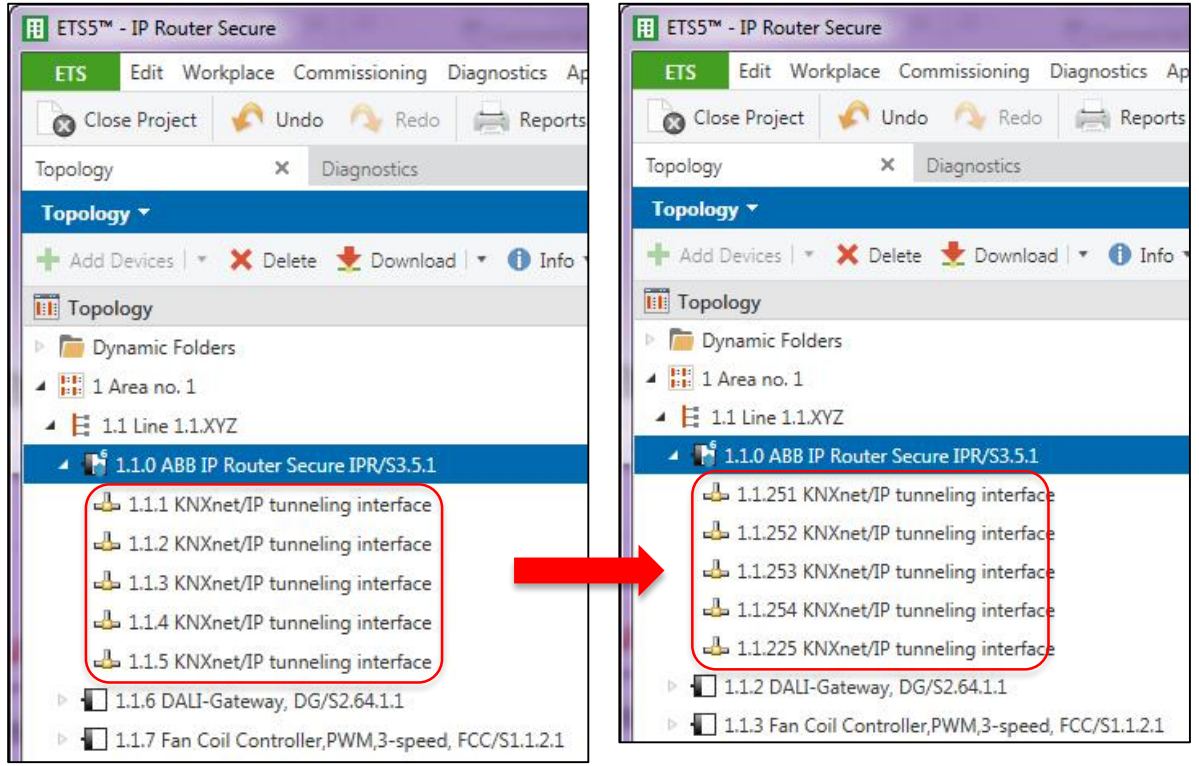
- The LED lights up continuously when the supply voltage Us is present and the Router is connected to KNX after the startup process is complete
- The LED flashes with data traffic on KNX



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Supplied state

- The device is supplied with the physical address 15.15.0
- All physical tunneling connection addresses are set to 15.15.100 in the supplied state (only one tunnel is visible to the outside)
- In ETS5, the first five free addresses in the line are assigned automatically after the IP Router has been inserted into a line
- The tunneling connection addresses set in the ETS will be adopted only after the first download
- The IP address is set to automatic IP assignment (DHCP/AutoIP)
- The device is supplied with the option “Group telegrams - Route”
  → This is not the default setting in the application, but it simplifies commissioning
- The parametrized settings will be adopted after the first download



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Market Introduction

– Market Launch: Q2/2019

Ident No.	Type	Status
2CDG 110 177 R0011	IPS/S 3.1.1 IP Interface	Available further on
2CDG 110 175 R0011	IPR/S 3.1.1 IP Router	Available further on
2CDG 110 176 R0011	IPR/S 3.5.1 IP Router Secure	New

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

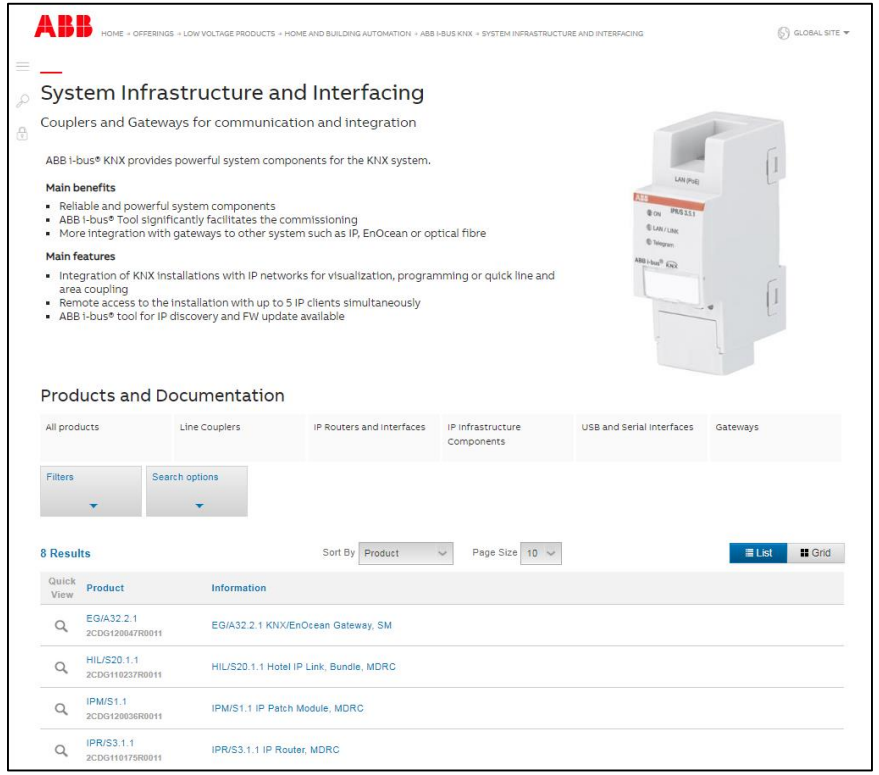
ABB IP Router Secure IPR/S 3.5.1 – Technical documents

www.abb.com/KNX

→ Products and Downloads

→ System Infrastructure and Interfacing

- Application Software ETS5
- Product Manual
- Technical Data
- Installation and Operating Instructions
- Specification Text
- Product Information
- Presentation Slides
- CE Declaration of Conformity (.PDF)
- Environmental Information
- …

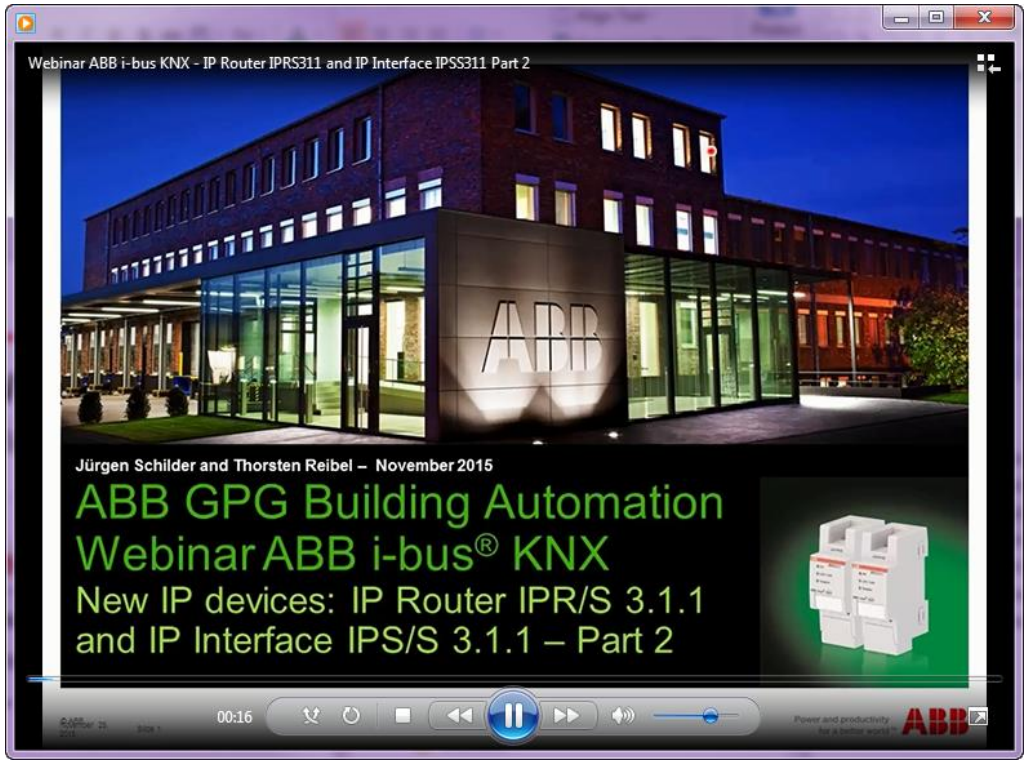


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Training

Training & Qualification Database: https://go.abb/ba-training

– Webinars
  - New IP devices: IP Router IPR/S 3.1.1 and IP Interface IPS/S 3.1.1 (October 2015)
  - Advanced features of IP devices: IP Router IPR/S 3.1.1 and IP Interface IPS/S 3.1.1 – Part 2 (November 2015)
  - Various software tools for KNX, e.g. firmware update with ABB i-bus® Tool (February 2019)
– Webinar slides
– Webinar recordings (MP4 file)



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1

- The IP Router Secure has the same properties (ETS parameter, filter table, …) as a standard IP Router
- NEW: For commissioning and operation in KNX Secure mode, the “Factory Default Setup Key” (FDSK) is also required
- When delivered, there are two stickers with the “Device Certificate” on the left side of the device
- No backdoor – if a project or the keys are lost, they are lost!

Device Certificate (FDSK)
AABL57-P7KAAA-
CAQDAQ-CQMBYI-
BEFAWD-ANBYHT
FDSK
AABL57-P7KAAA-
CAQDAQ-CQMBYI-
BEFAWD-ANBYHT

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

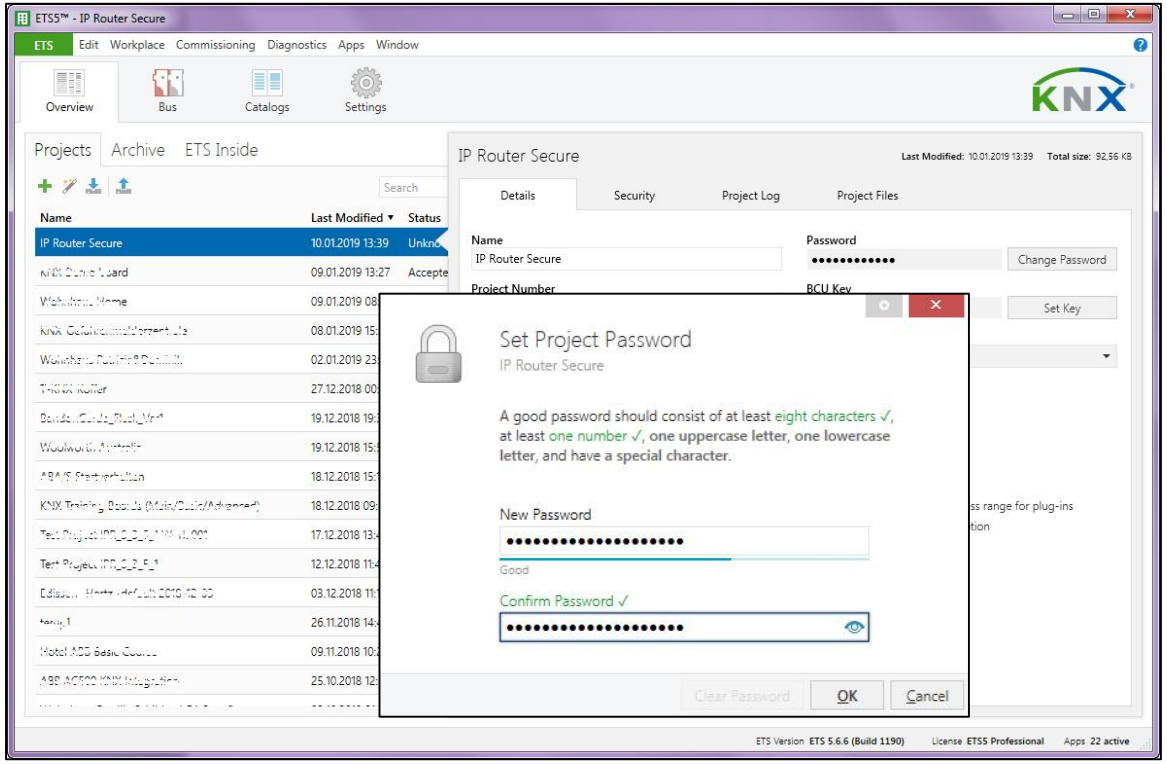
ABB IP Router Secure IPR/S 3.5.1

- When commissioning the device, therefore, a few points must be considered
- Only ETS5 is supporting KNX Secure
- Manufacturers of BMS/visualization software have integrated KNX Secure, so interoperability with IP Router Secure is available

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

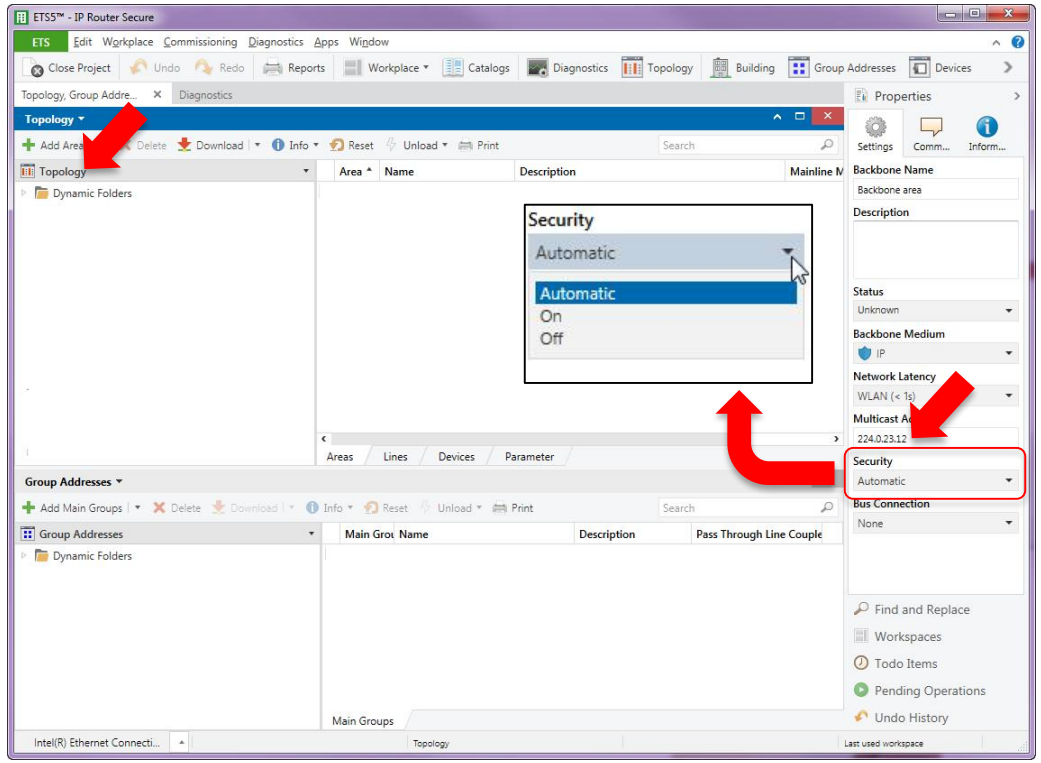
- As soon as a KNX Secure device is imported into a project, an ETS project password must be assigned
  → ETS enforces this
- The project is thus protected against unauthorized access
- The password must not be lost – without this password, access to the project is not possible



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

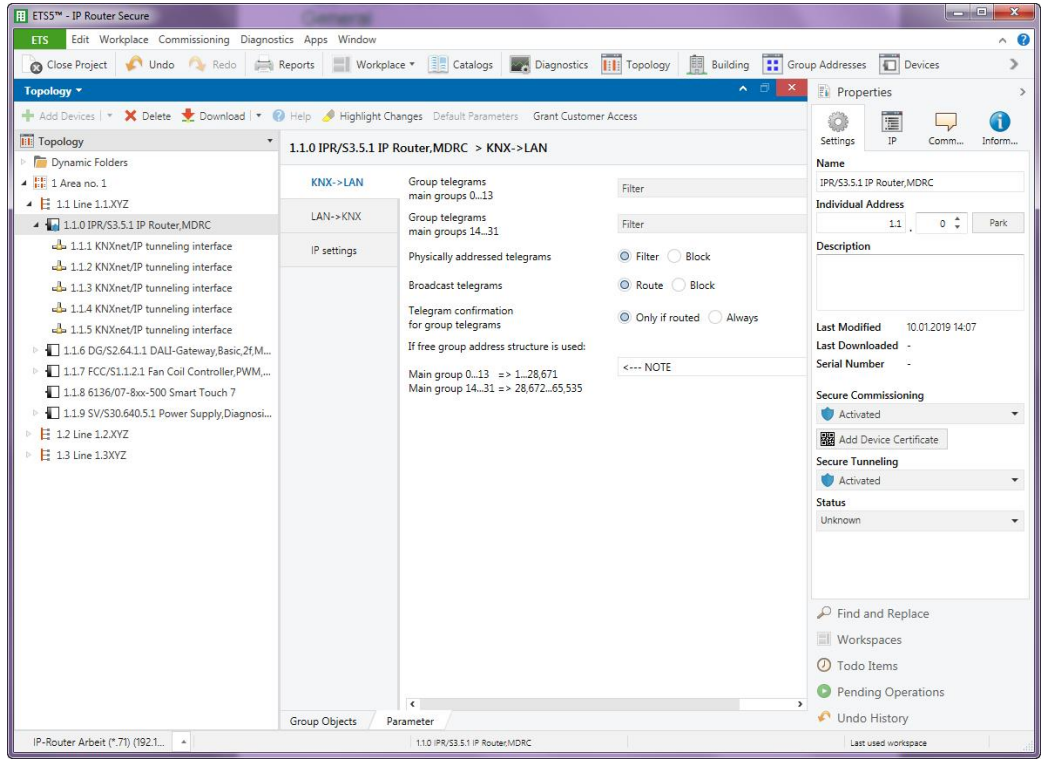
– In the topology view, set the security level
  - Automatic (default)
  - ON
  - OFF



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

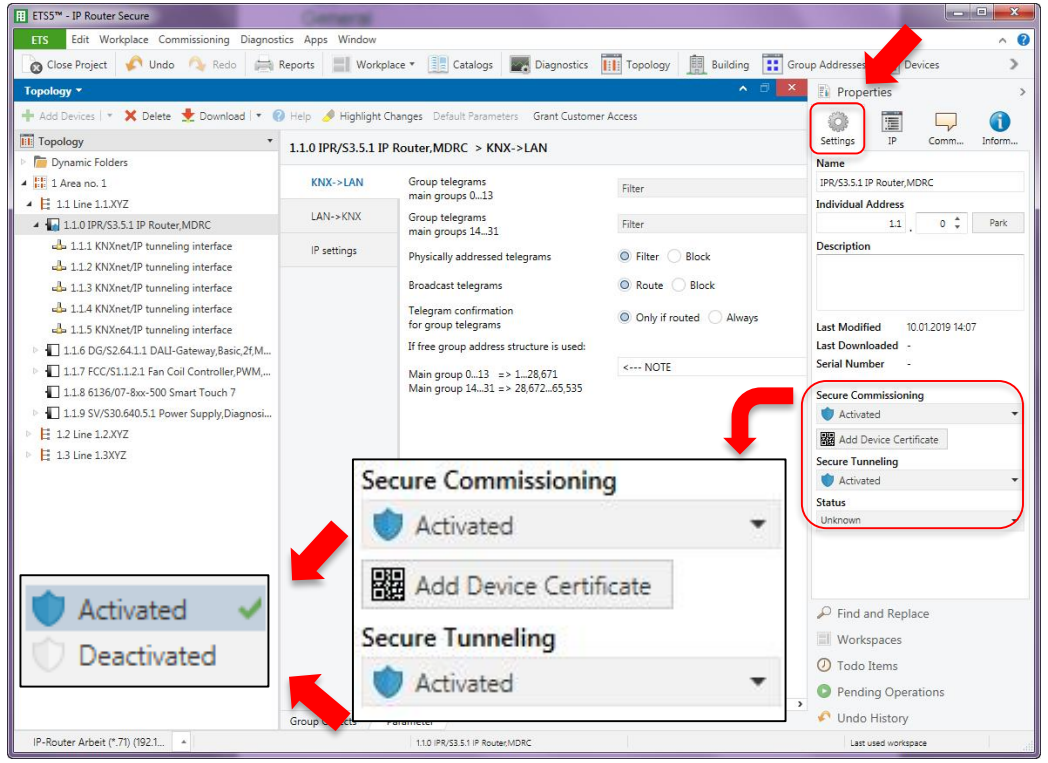
- Add IP Routers Secure and the other devices to the project, set parameters, link group addresses ,…
- IP Routers Secure have the same parameters (filter table, …) as a standard IP Routers
- Additional addresses (local) for the tunneling server of the IP Router are defined



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

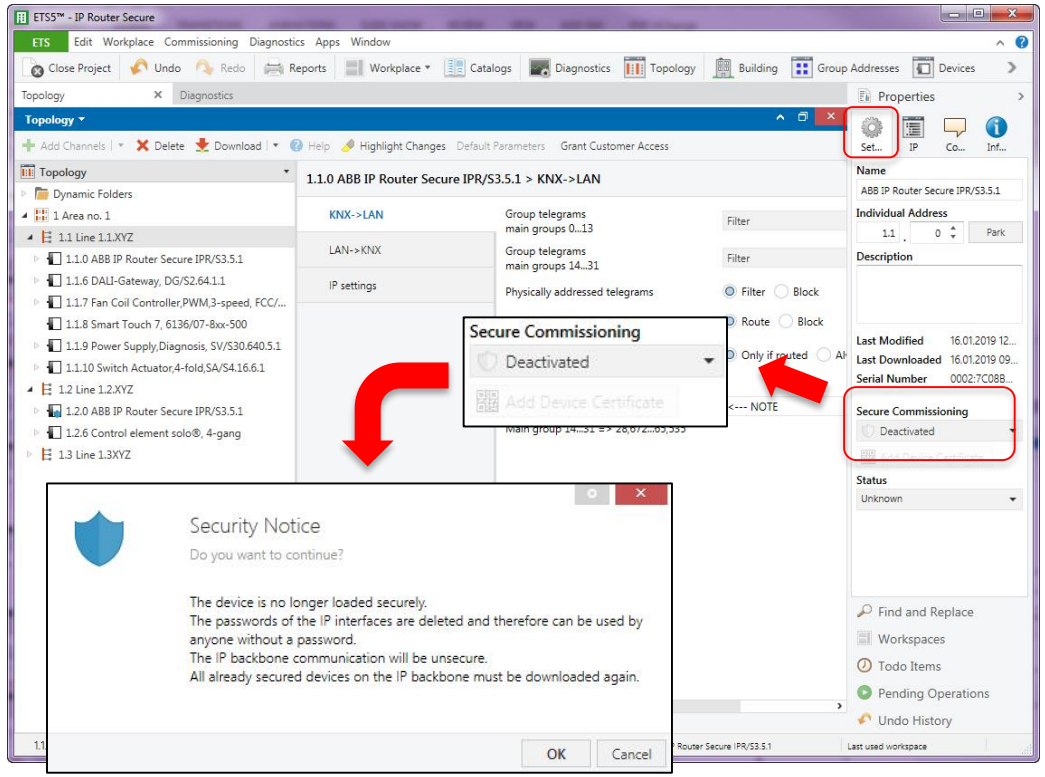
- “Properties” → “Settings”
  - Device name (is loaded in the device)
  - Individual address
  - Description
- New:
  - Secure Commissioning
  - Add device certificate (FDSK and serial number)
  - Secure Tunneling



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

- “Properties” → “Settings”
- Secure Commissioning
  - If secure commissioning is deactivated for at least one IP router, all IP Router Secure and the communication on the IP backbone is not in secure mode!!!



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

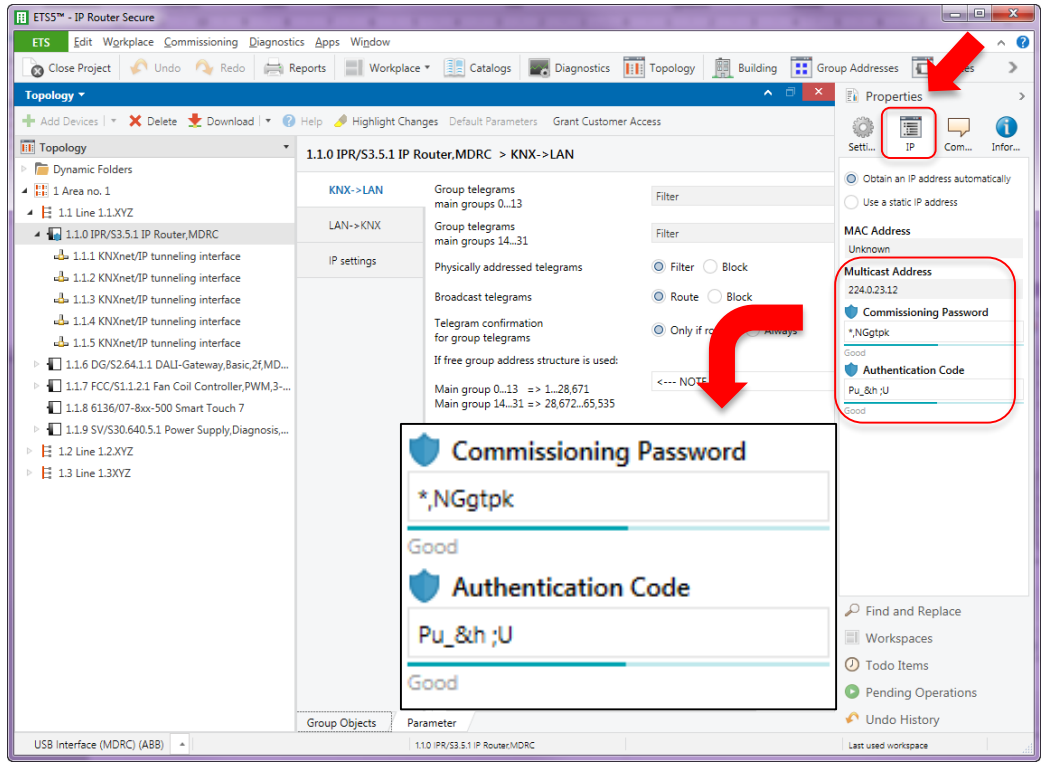
ABB IP Router Secure IPR/S 3.5.1 – Commissioning

– “Properties” → “IP”

- Setting the IP address (automatically or static)
- Multicast address
  224.0.23.12 / port 3671 is the defined address for the KNXnet/IP from the KNX Association in conjunction with IANA for KNX IP devices
- The MAC address is read out after a download and displayed

New:

- Commissioning password
- Authentication code

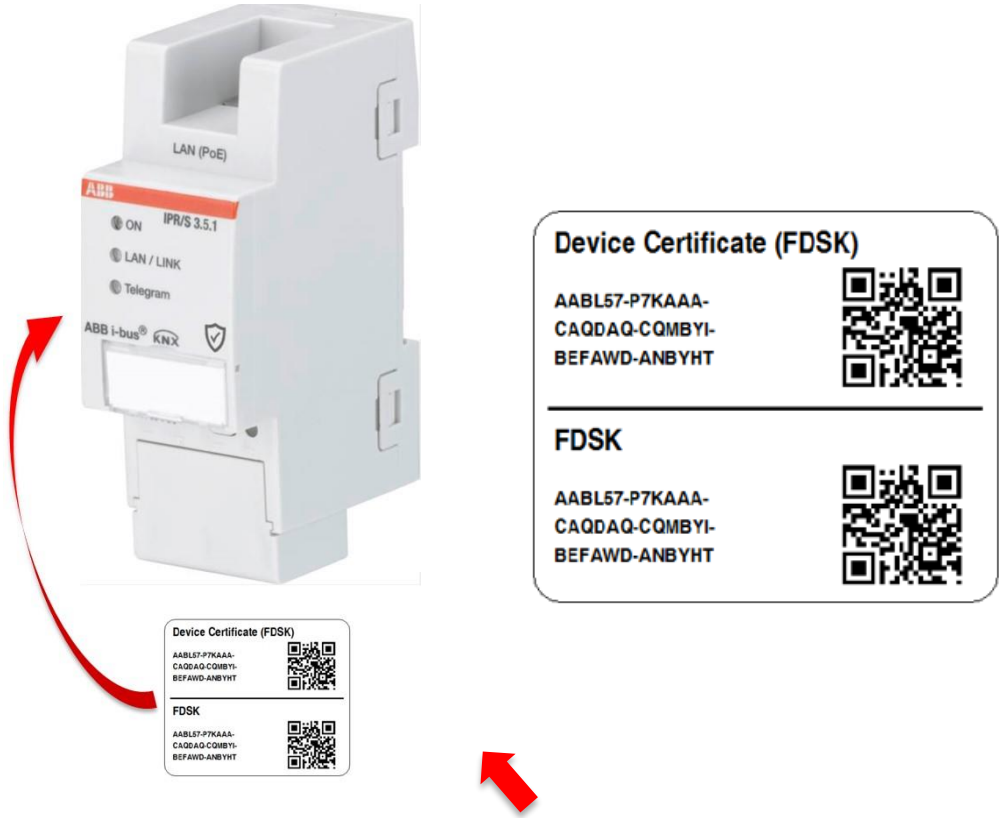


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

- When commissioning a KNX secure device (first download), a commissioning key (“Device Certificate”) is required
- This commissioning key consists of
  - FDSK = Factory Default Setup Key
  - Serial number IPR/S

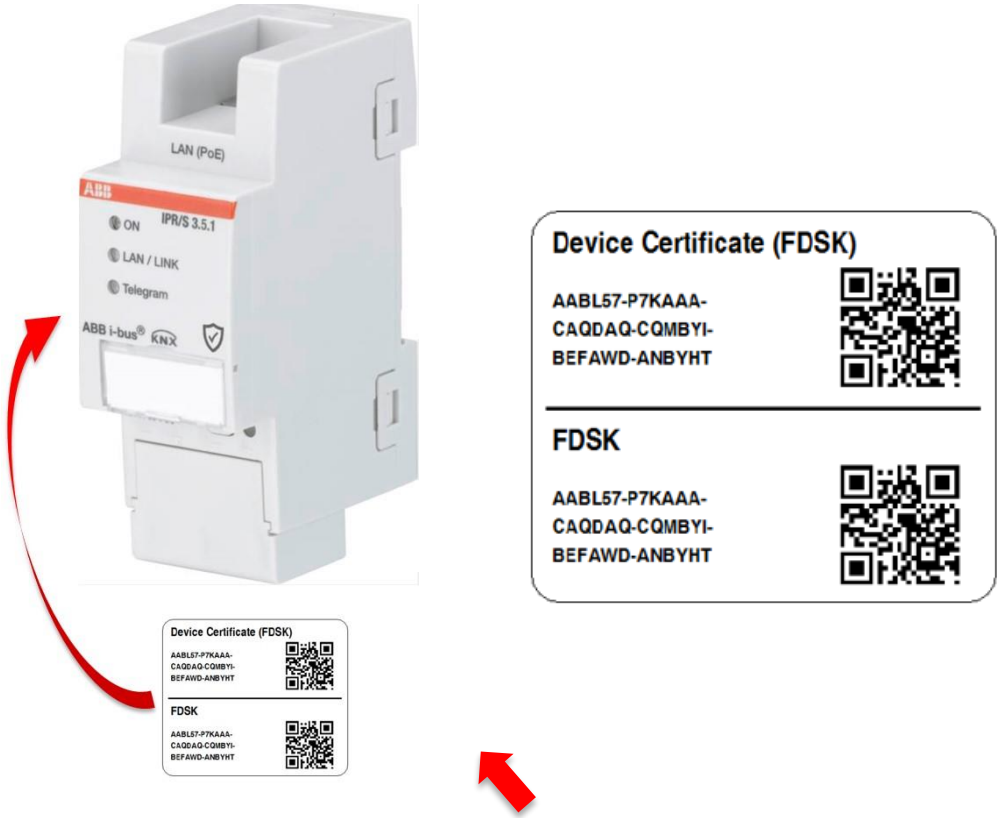
  and is placed on a sticker on the left side of the device and must be imported into the ETS
- One sticker can be used for project documentation, the other can be left on the device



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

- The FDSK is only required for initial commissioning
- After that, the ETS creates new “Tool Keys”
- The “Tool Keys” are transferred via the bus with encryption based on FDSK to the IP Routers
- Further device configuration is encrypted based on the “Tool Key”
- The FDSK is only needed again after a device reset to factory settings

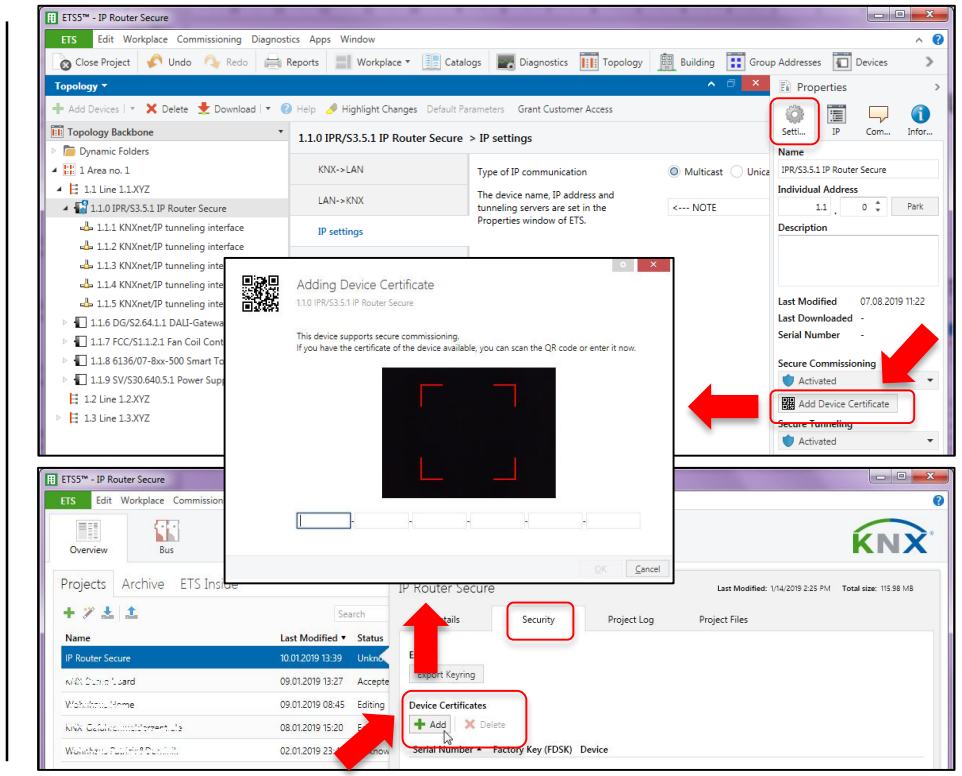


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

How to enter the “Device Certificate”?

- The ETS asks for the key when first programming
- Click on “Add Device Certificate”
  - Selected device
  - ETS main menu “Security”
- The reading can be done offline
- The keys are assigned automatically to the IP Routers Secure by ETS

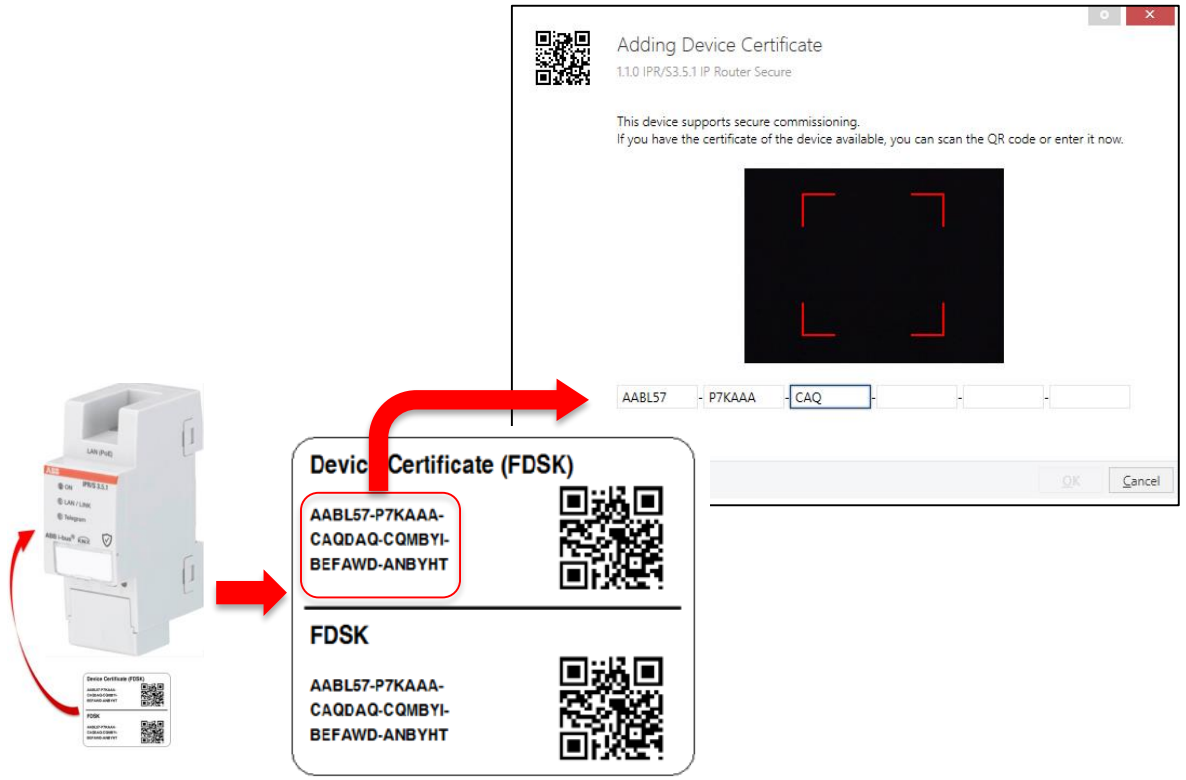


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

How to enter the “Device Certificate”?

– The key can be
  - Entered via the keyboard
  - Read in with a QR code scanner
  - Read with the webcam of laptop



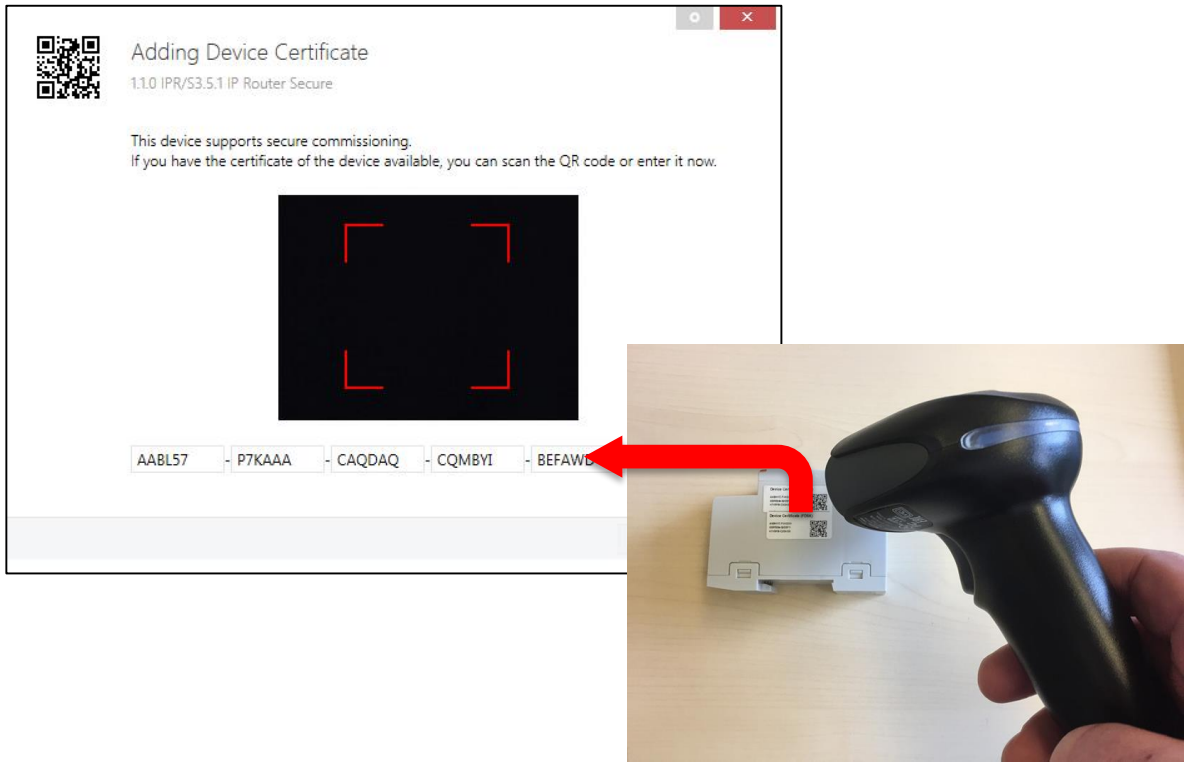
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

How to enter the “Device Certificate”?

– The key can be

- Entered via the keyboard
- Read in with a QR code scanner
- Read with the webcam of laptop

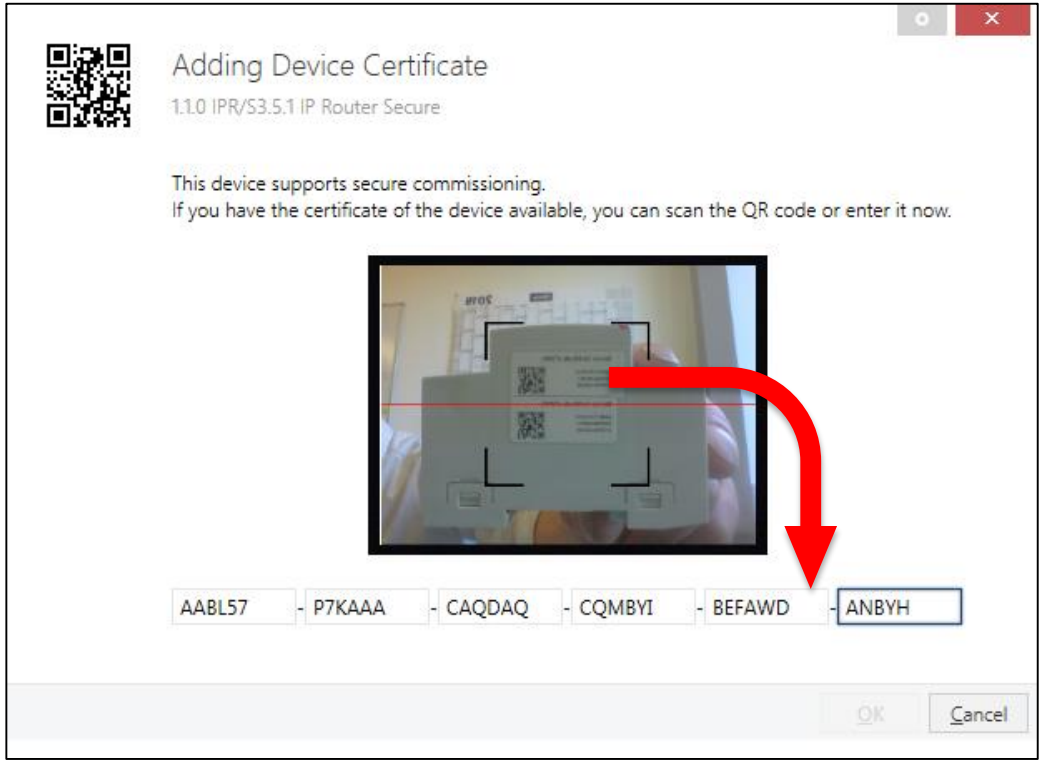


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

How to enter the “Device Certificate”?

– The key can be
  - Entered via the keyboard
  - Read in with a QR code scanner
  - Read with the webcam of laptop

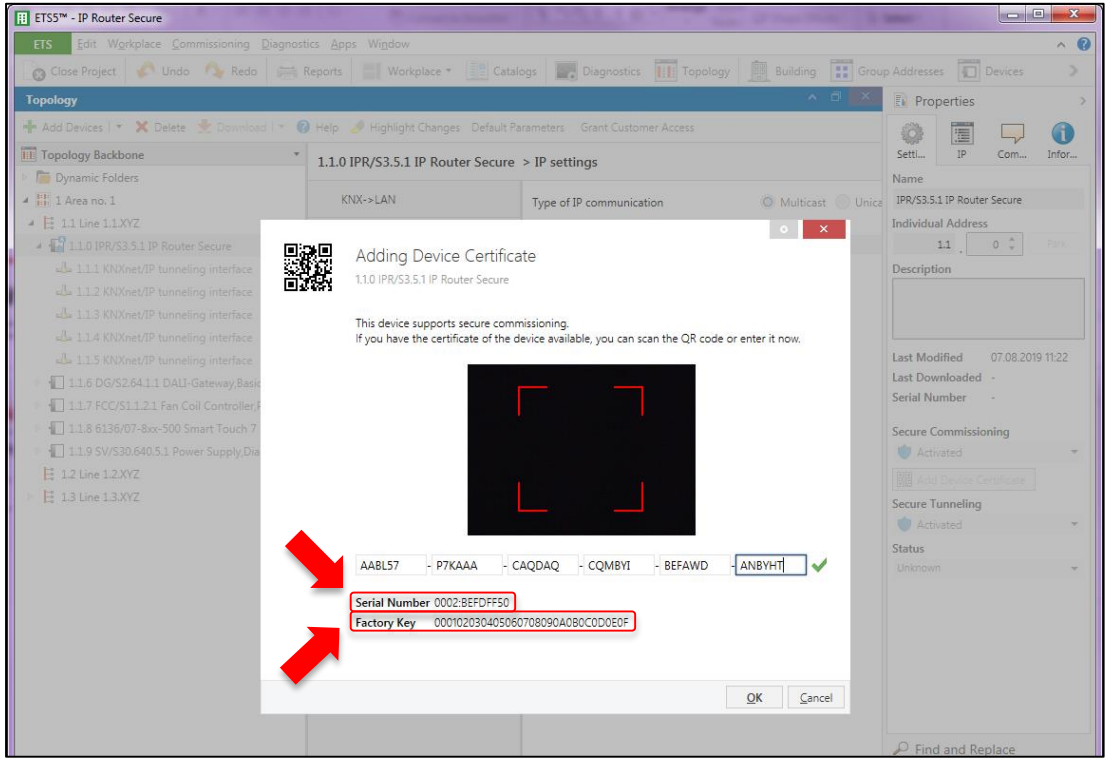


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

How to enter the “Device Certificate”?

- Valid keys (serial number and FDSK) has been entered
- The ETS assigns the FDSK to the IP Routers Secure automatically



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Commissioning

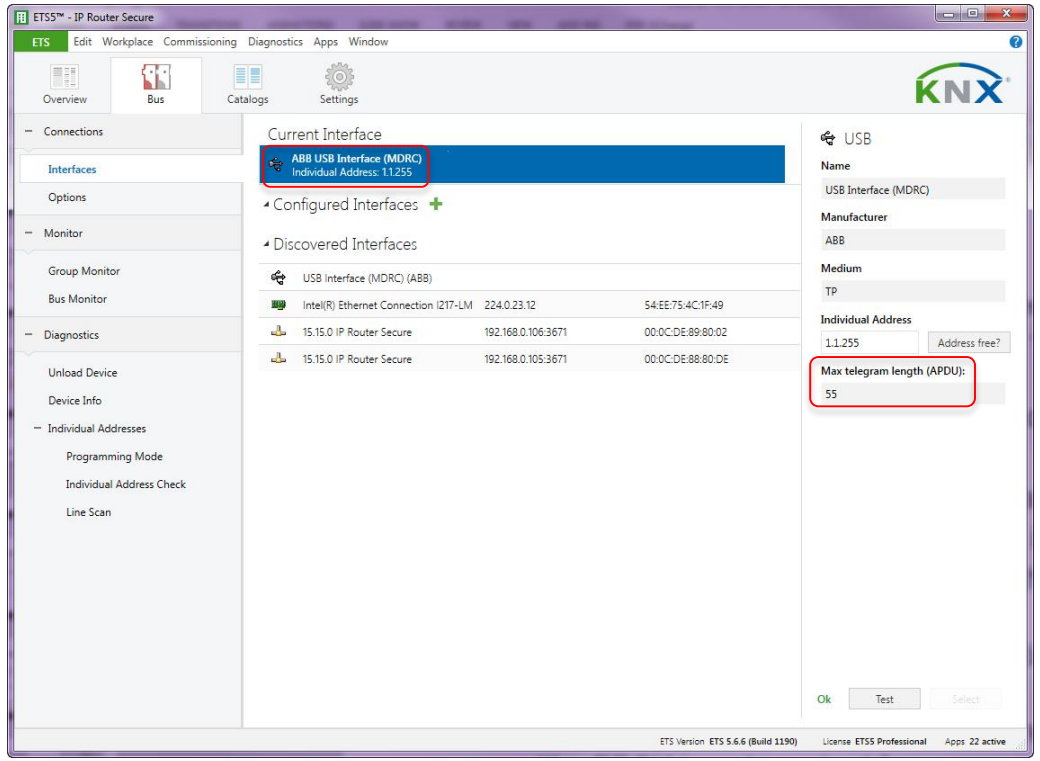
- The ETS assigns the “Backbone Key” to all KNX IP Secure devices in the project and also generates separate passwords for each tunneling server
- The passwords of the tunneling server can be changed if necessary
- The keys are generated and managed by the ETS
- If necessary, keys and passwords can be exported

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Download IP Router Sec.

The individual address and application program can be programmed in different ways

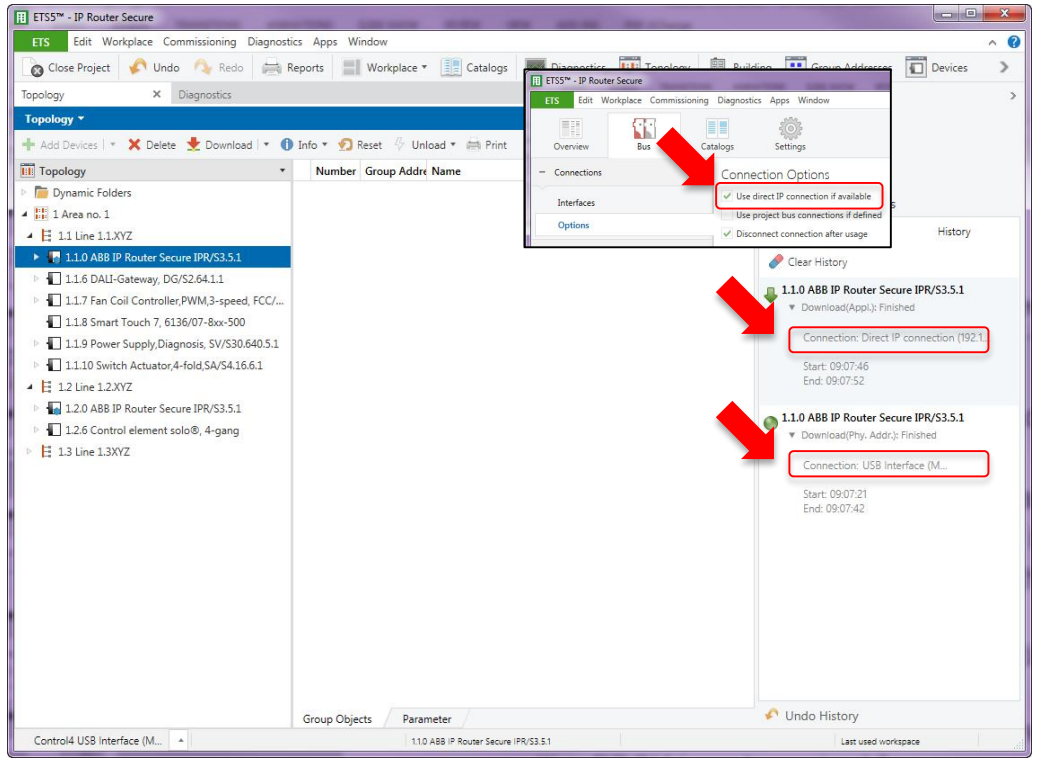
- Another programming interface (USB or IP) which supports KNX “long frame” telegrams (APDU > 15), e.g. USB/S 1.2 from ABB
- One of the integrated tunneling servers
- Local download, via KNXnet/IP Routing



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Download IP Router Sec.

- The individual address was programmed via USB
- Even though another interface, e.g. USB is used, the ETS switches to “Direct IP” and the application program will be downloaded directly via IP (if “Use direct IP connection" is activated and the IP connection is available)



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

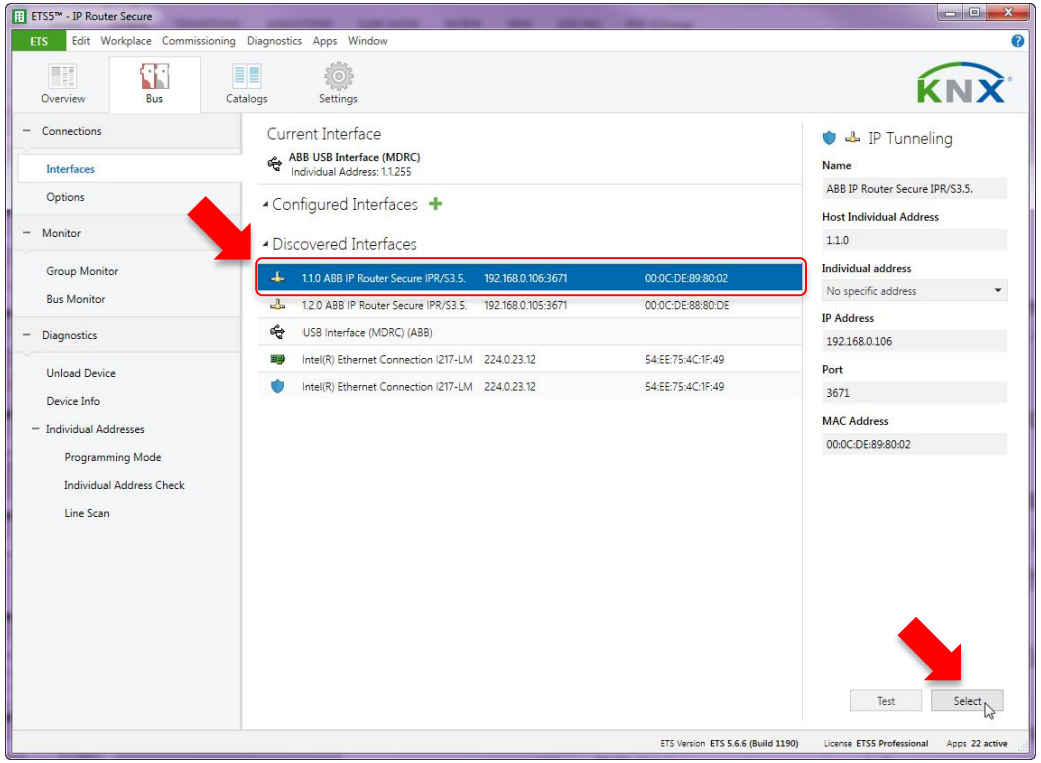
ABB IP Router Secure IPR/S 3.5.1 – Downloading

Downloading with tunneling servers:

With one of the integrated tunneling connections KNX devices and the IP Router Secure can be programmed

– Choose the tunneling interface of an IP Router and click “Select”

– …



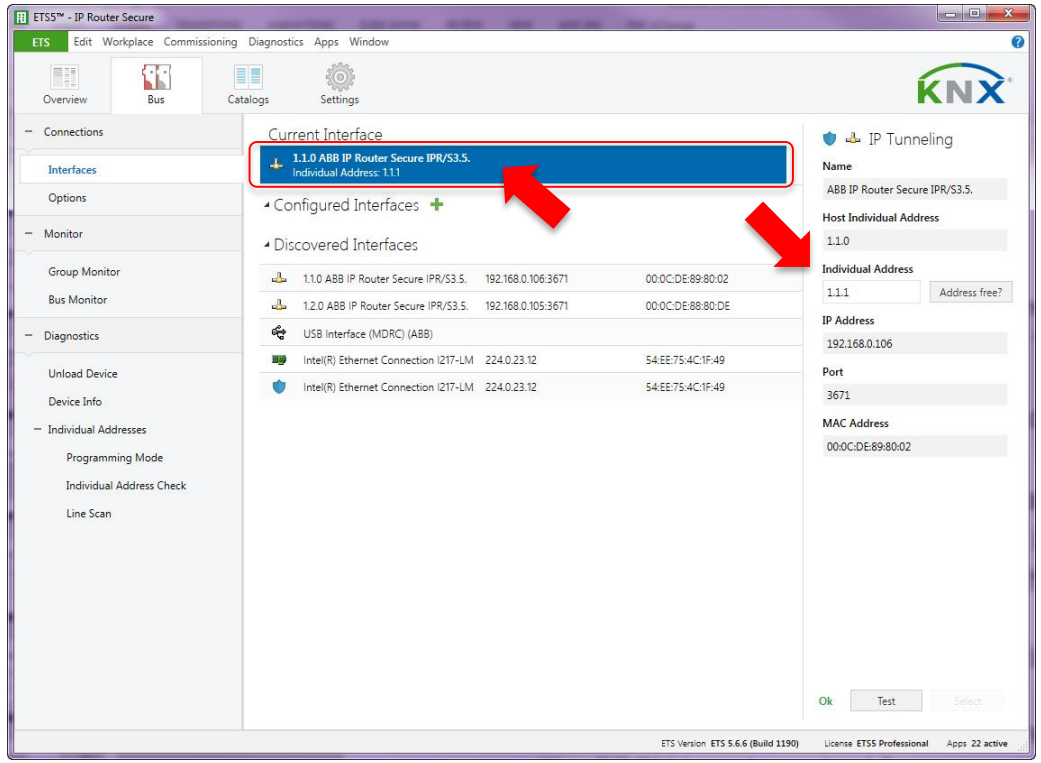
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Downloading

Downloading with tunneling servers:

With one of the integrated tunneling connections KNX devices and the IP Router Secure can be programmed

- …
- One of the free tunneling servers will be taken over
- For a faster download, a tunnel connection should be created to each IP Router Secure



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

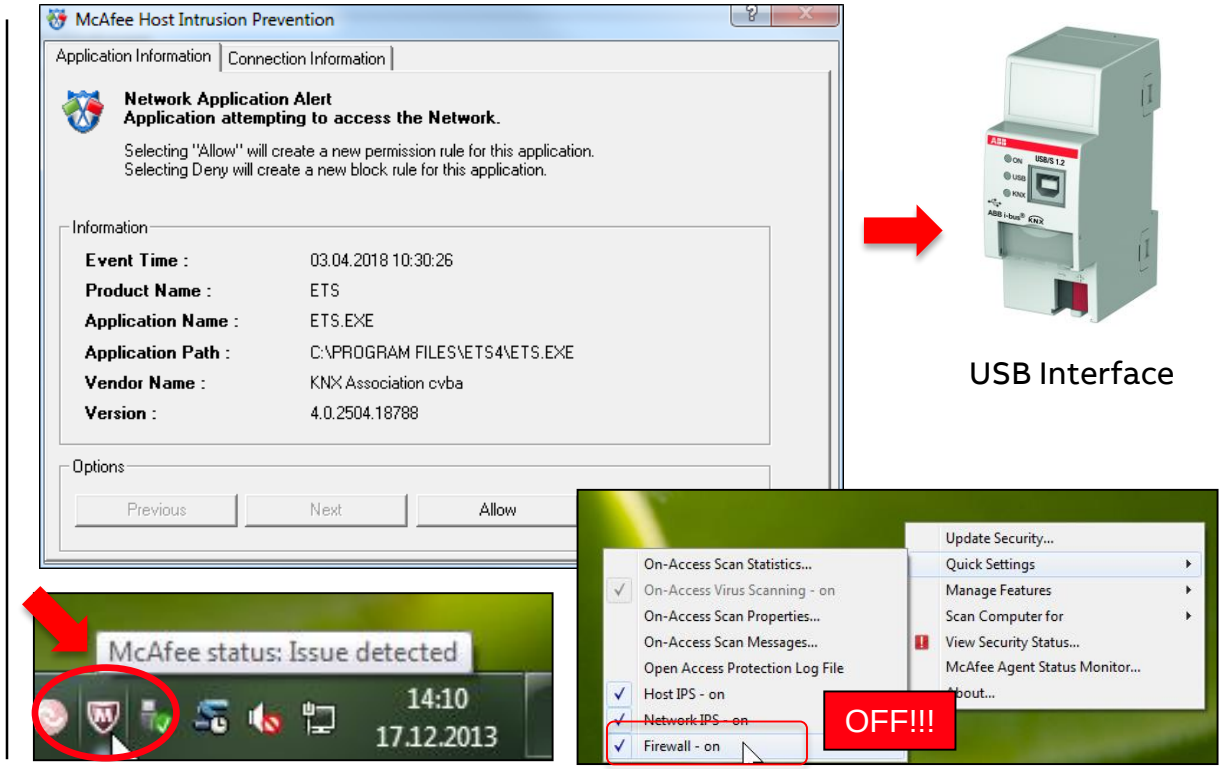
ABB IP Router Secure IPR/S 3.5.1 – Downloading

Downloading with tunneling servers:

With one of the integrated tunneling connections KNX devices and the IP Router Secure can be programmed

– Firewall, virus scanner, … can block a download

→ USB Interface!

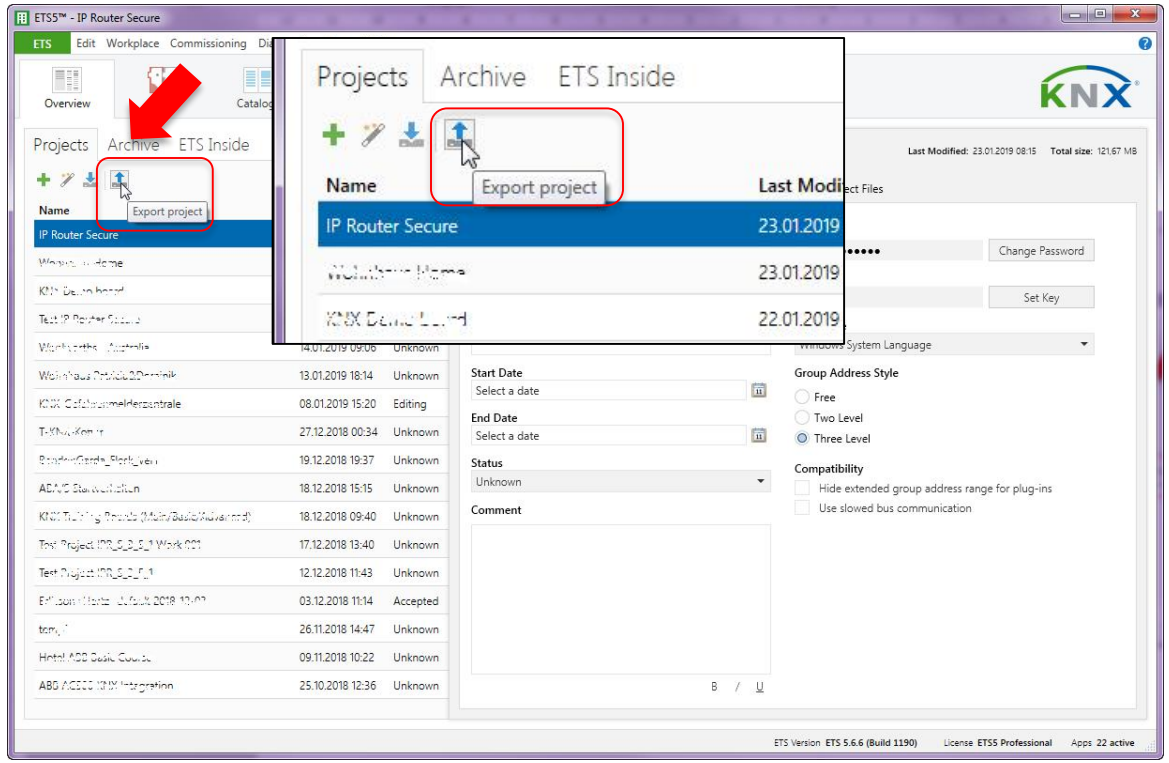


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Export

Export of ETS project:

- Projects should be exported at regular intervals
- The exported projects are quasi the “backups” on which one can fall back later on
- The completely exported project contains additional files
  - DLLs of plug-ins
  - KNX Secure passwords, keys, …

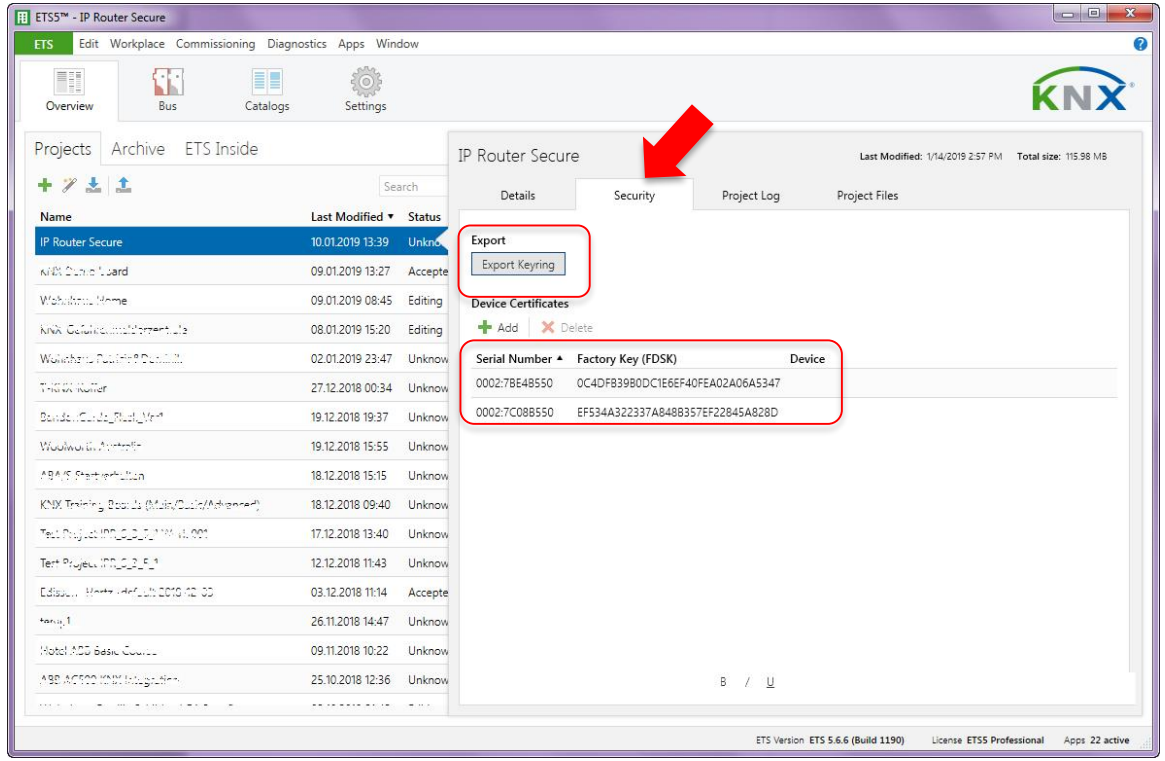


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Export

Export all KNX Secure keys, passwords, …:

- ETS main menu “Security” → Export of all keys “Keyring”
  - Backup
  - For visualization systems based on this project
  - Diagnostics with another ETS
- Password protected file “*.knxkeys”

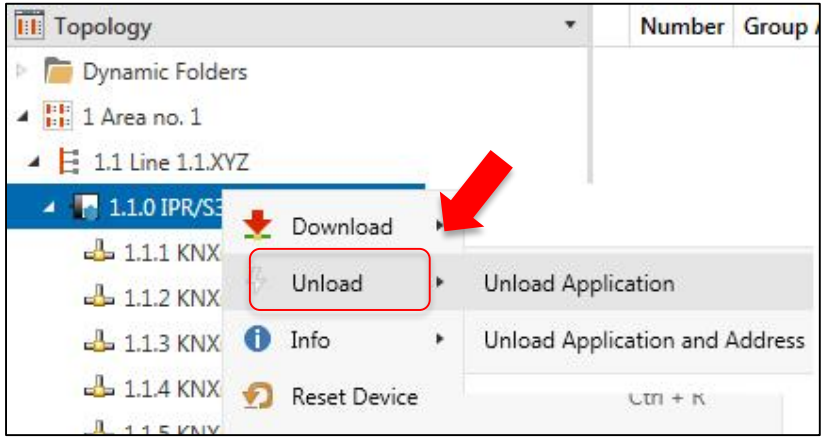


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Reset

Unload the IP Router Secure and reset to factory settings:

- The device can be reset to factory settings
- It is a secure device and the following should be noted:
  - In secure mode operation, the device can only be reset via the ETS if the ETS uses the project with which the device was parameterized or if the FDSK is present in the project
  - The IP Router Secure will be unloaded like a standard device



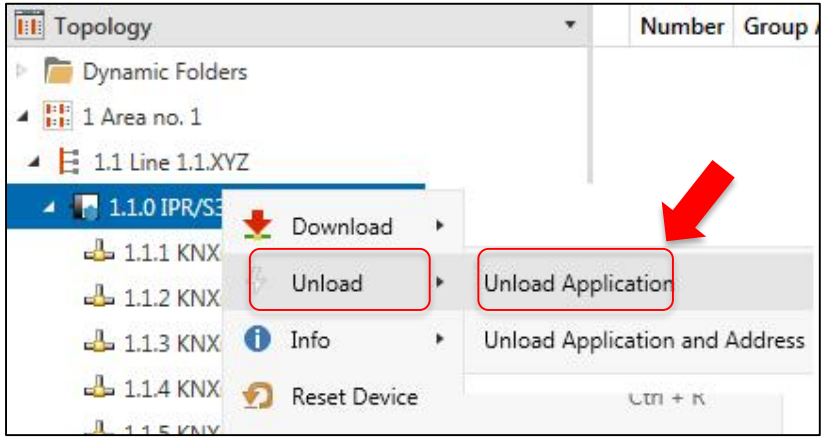
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Reset

Unload the IP Router Secure and reset to factory settings:

Option “Unload application”

- The IP address and IP configuration will be retained
- Any unicast configuration will be retained
- The passwords and IP addresses of the tunneling servers will be deleted
- The key for multicast communication (“backbone key”) will be retained
- The tool key assigned by the ETS will be retained – the FDSK will not be needed for reprogramming
- The physical address will be retained



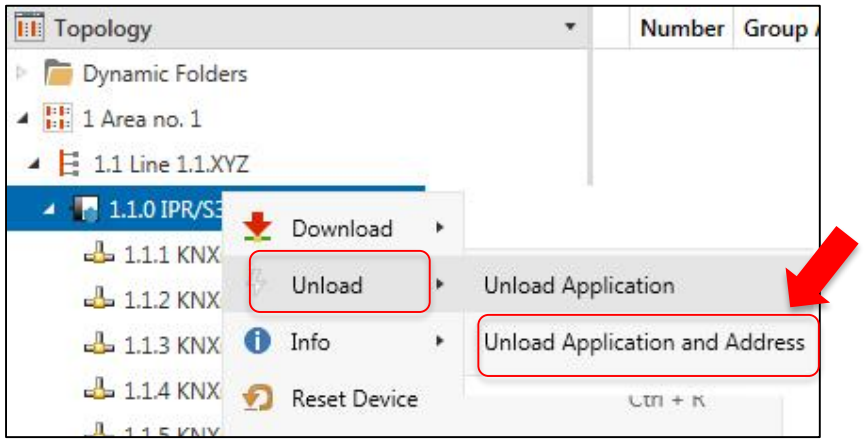
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Reset

Unload the IP Router Secure and reset to factory settings:

Option “Unload application and address”

- The device is reset to factory settings
  e.g. “Backbone Key”, “Tool Key”, … is deleted
- The FDSK is necessary for the recommissioning if it is not present in the ETS project from the original commissioning



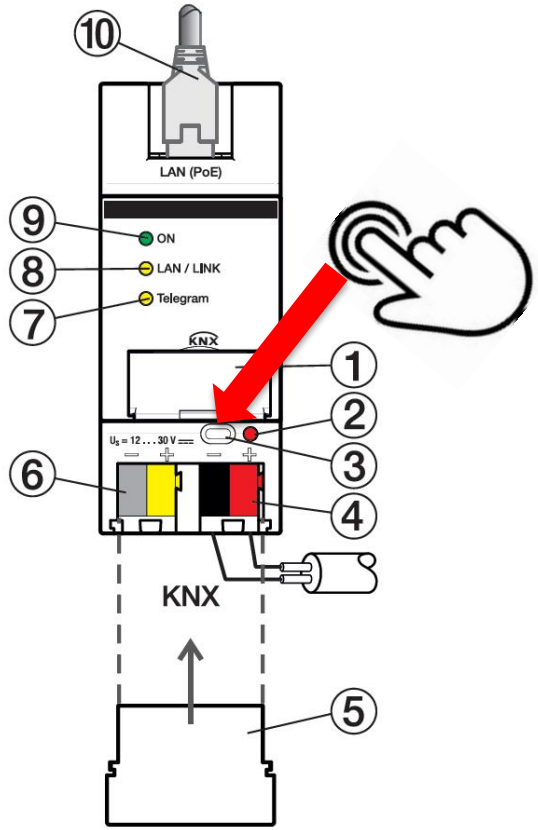
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – Reset

Reset directly on the IP Router Secure:

The reset to factory settings can also be performed directly on the device. This does not pose a security risk because the device is no longer part of the secure system → No multicast communication to other IP Router Secure possible!!!

- Press the programming button (3) when the KNX bus is not connected
- Hold the programming button (3) down and plug on the bus terminal
- The programming LED (2) flashes (2 Hz)
- Hold the programming button (3) for at least 5 sec. and then release it
- The programming LED (2) goes out, and the device reboots with the factory settings
- The IP Router can be reprogrammed if the device’s FDSK key is still known to the ETS

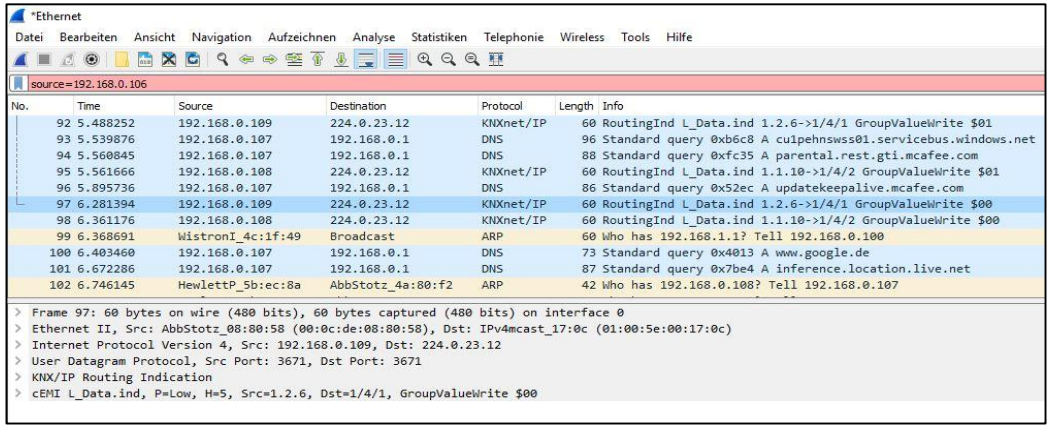


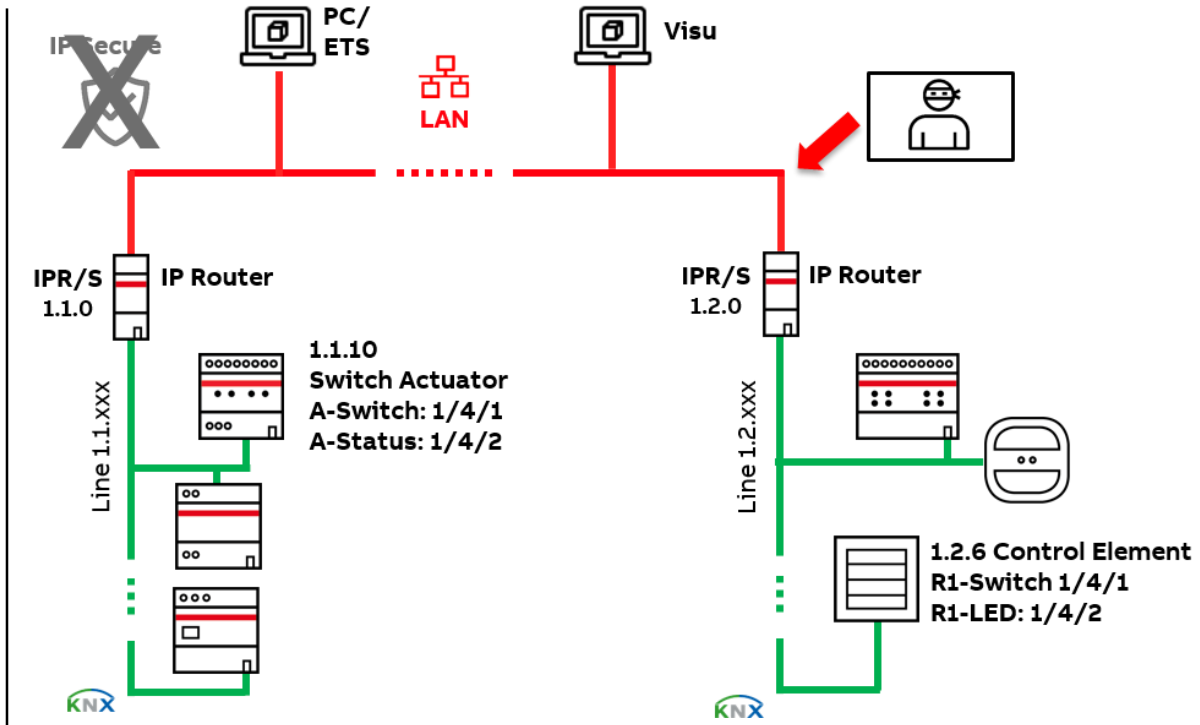
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Situation 1 – Attack over the IP network

No IP Secure

- Record and send KNX telegrams with ETS group monitor
- Record and analyze IP telegrams with special software, e.g. Wireshark

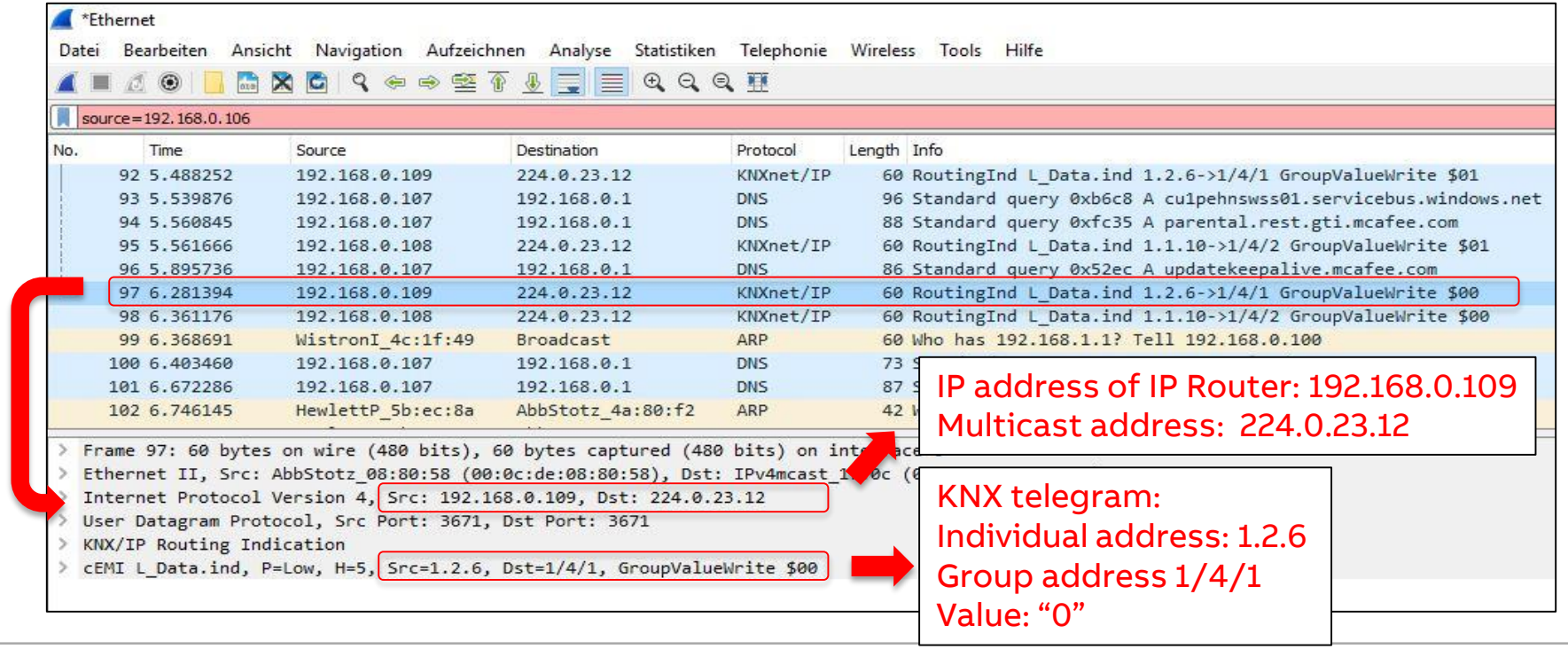




Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Situation 1 – Attack over the IP network

No IP Secure: Record and analyze IP telegram with special software, e.g. Wireshark

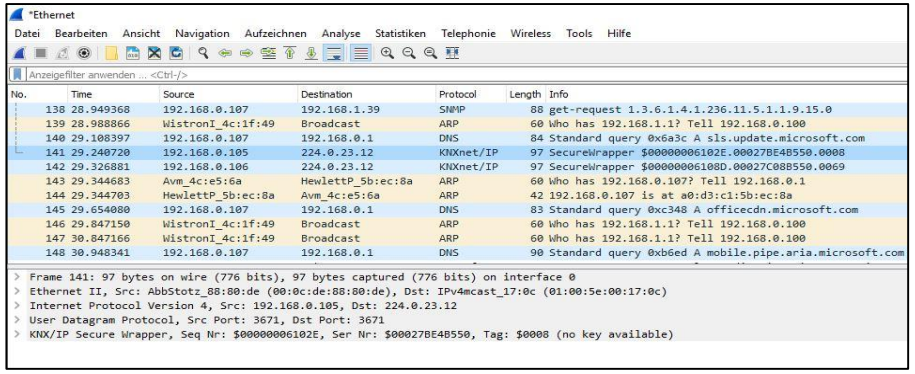


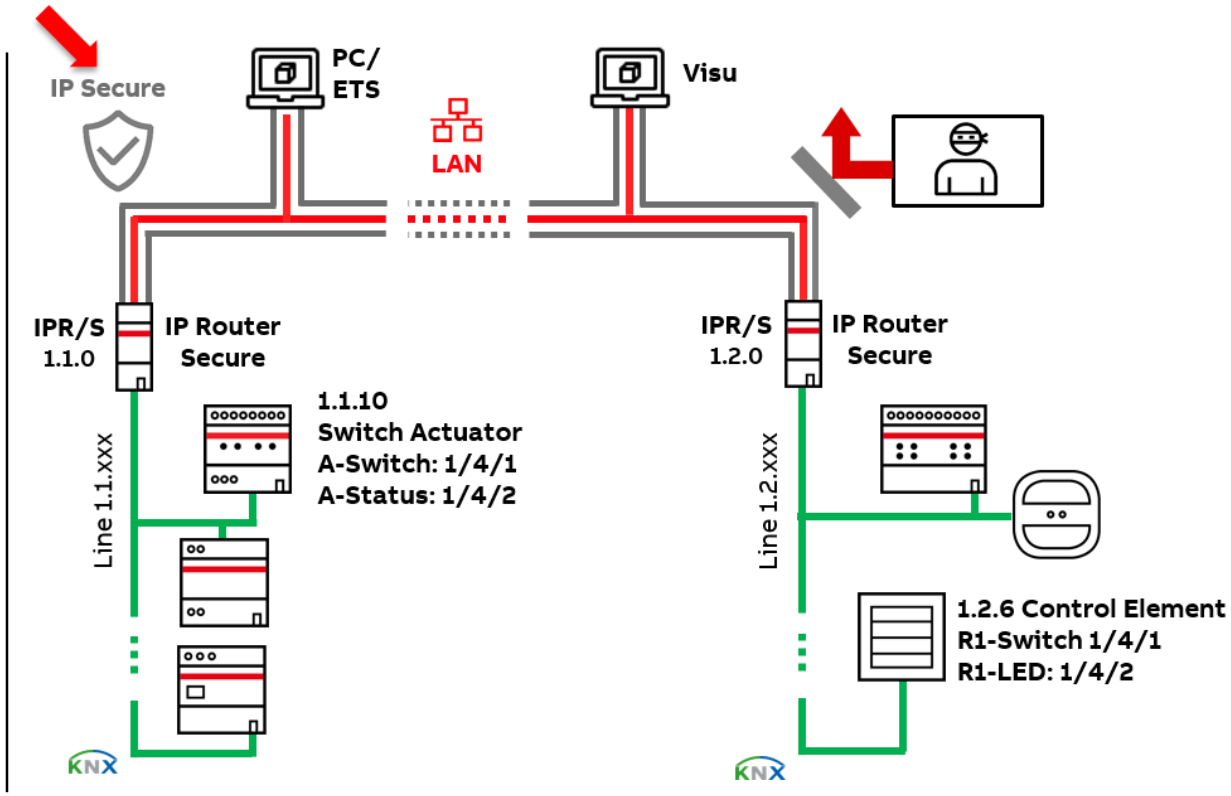
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Situation 2 – Attack over the IP network

IP Secure

- The complete KNX telegram is encrypted
- An IP telegram with the same KNX group address and the same value is different for each transmission
  → No replay attack possible!
- The ETS has assigned a “Backbone Key” for multicast communication on IP to all KNX IP Secure devices in the project

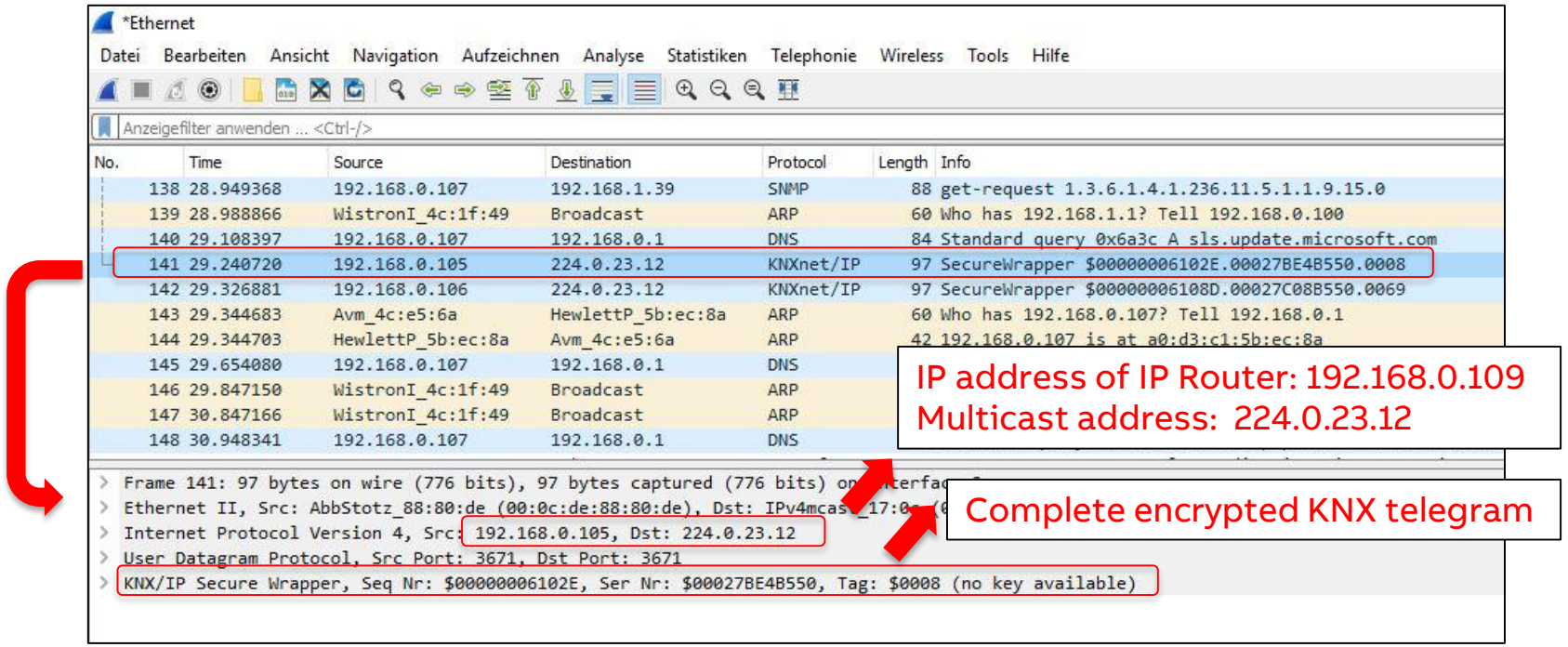




Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Situation 2 – Attack over the IP network

IP Secure: The complete KNX telegram is encrypted

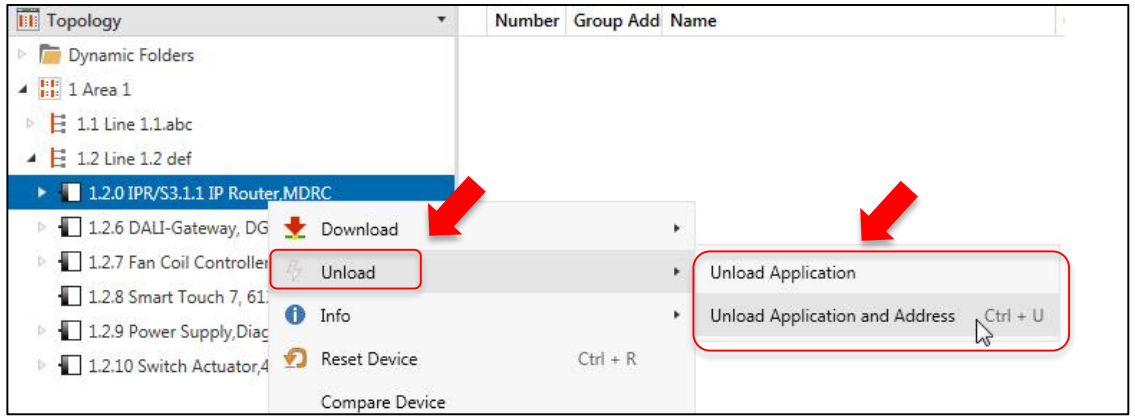


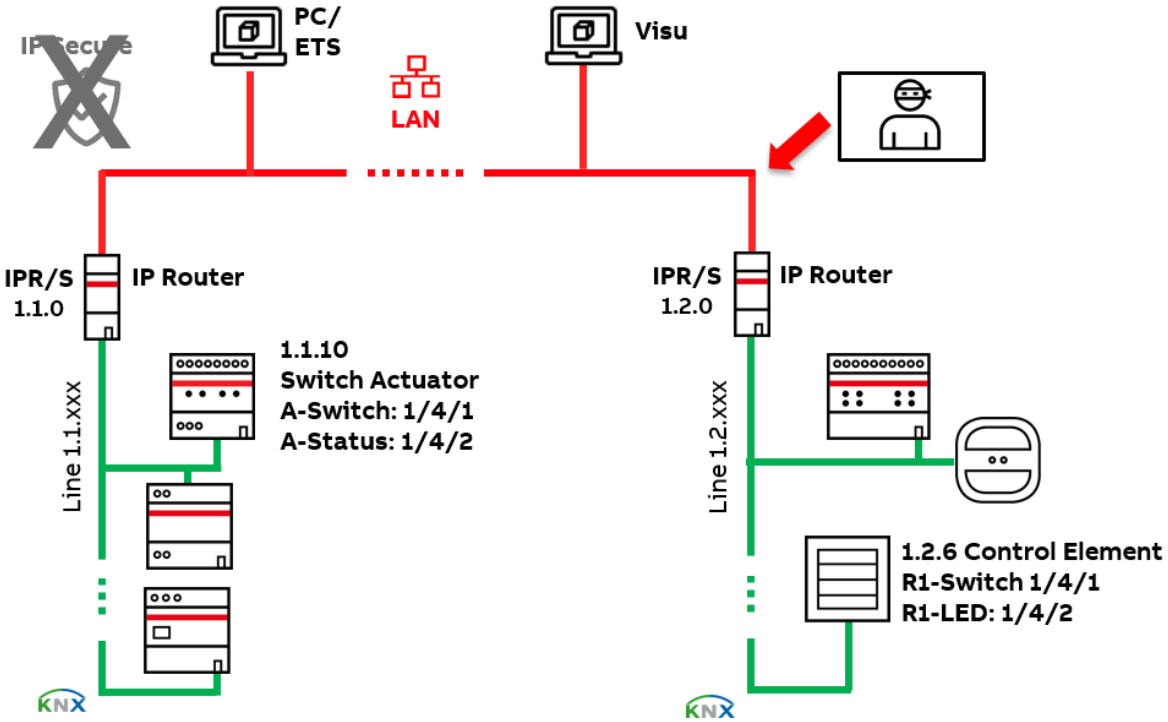
Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Situation 3 – Attack over the IP network

No IP Secure

– Unload and download an IP Router with the ETS is possible



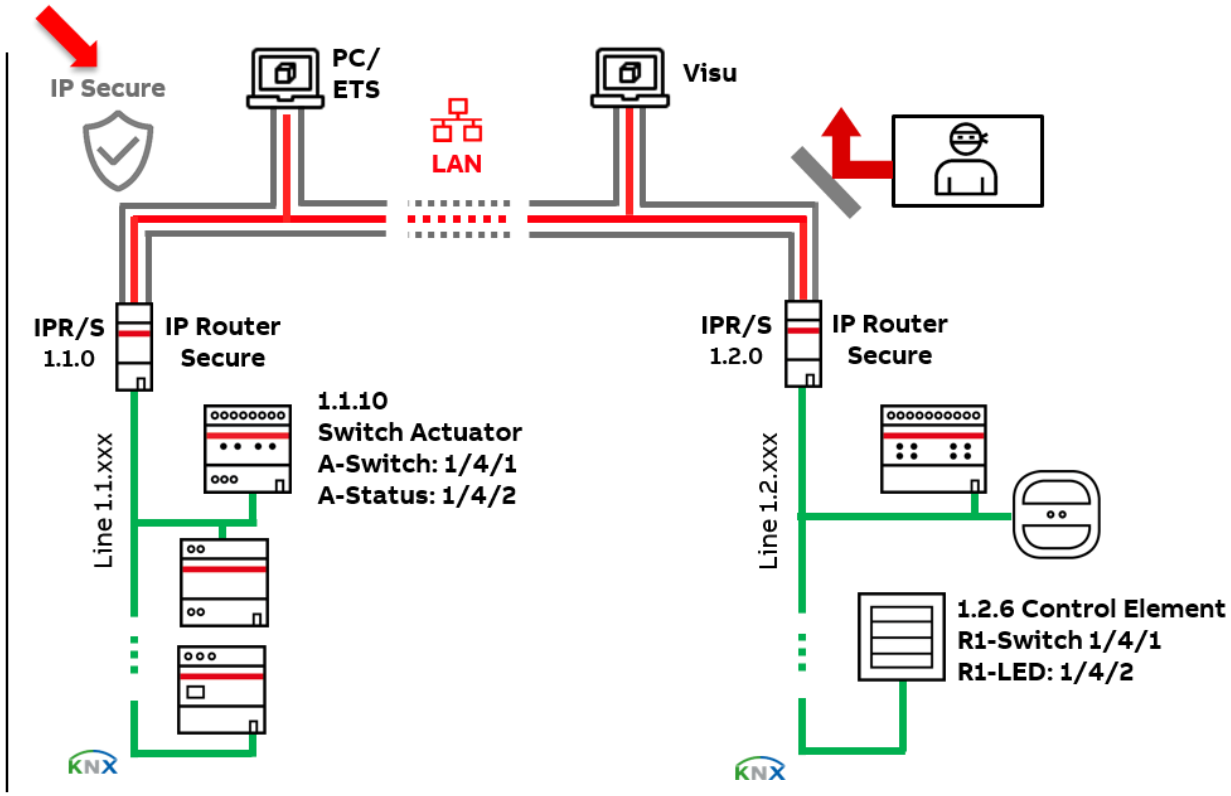


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Situation 4 – Attack over the IP network

IP Secure

– Unload and download an IP Router with an “Attack ETS” is not possible
→ No “Backbone Key”!

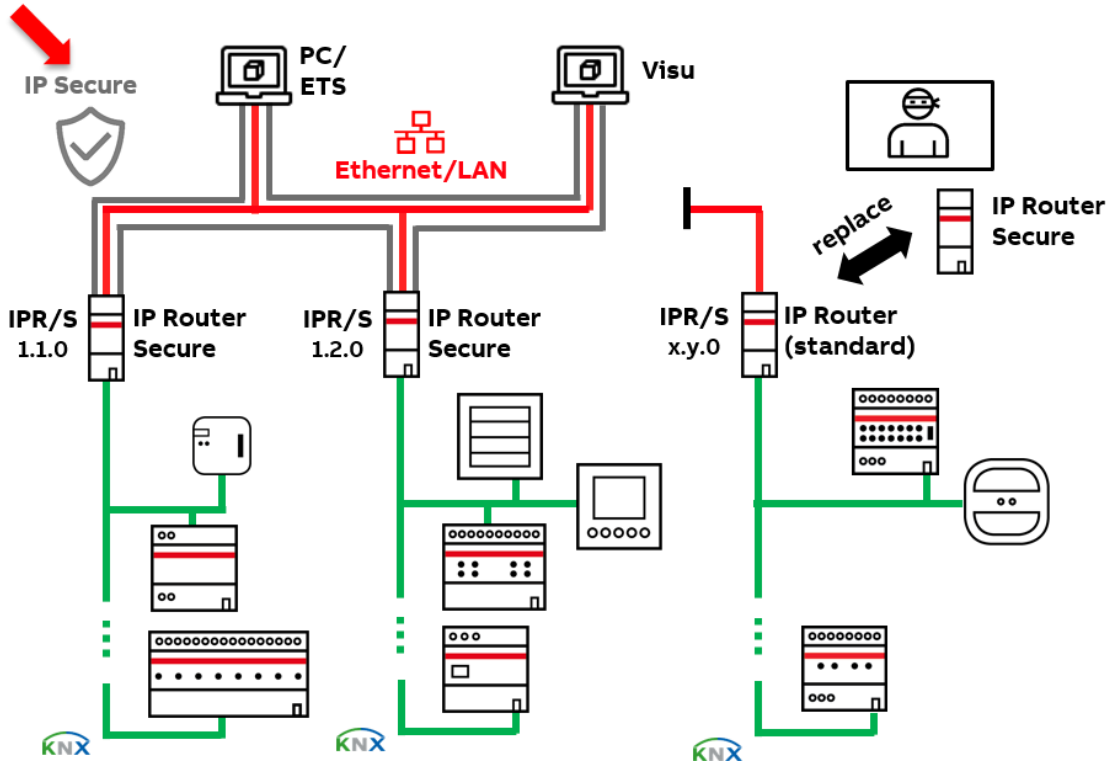


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Situation 5 – Attack over the IP network

IP Secure

- Replacing the IP Router Secure with a IP Router Standard
- This does not pose a security risk because the device is not a part of the secure system → No multicast communication to other IP Router Secure possible!!!

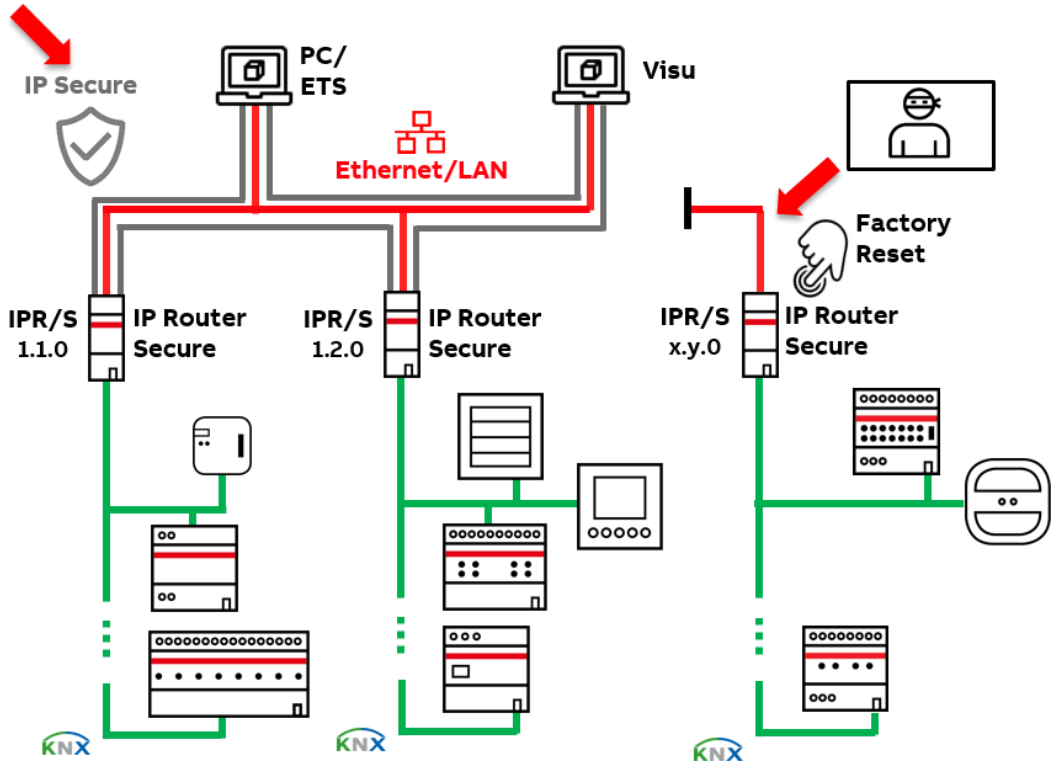


Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Situation 6 – Attack over the IP network

IP Secure

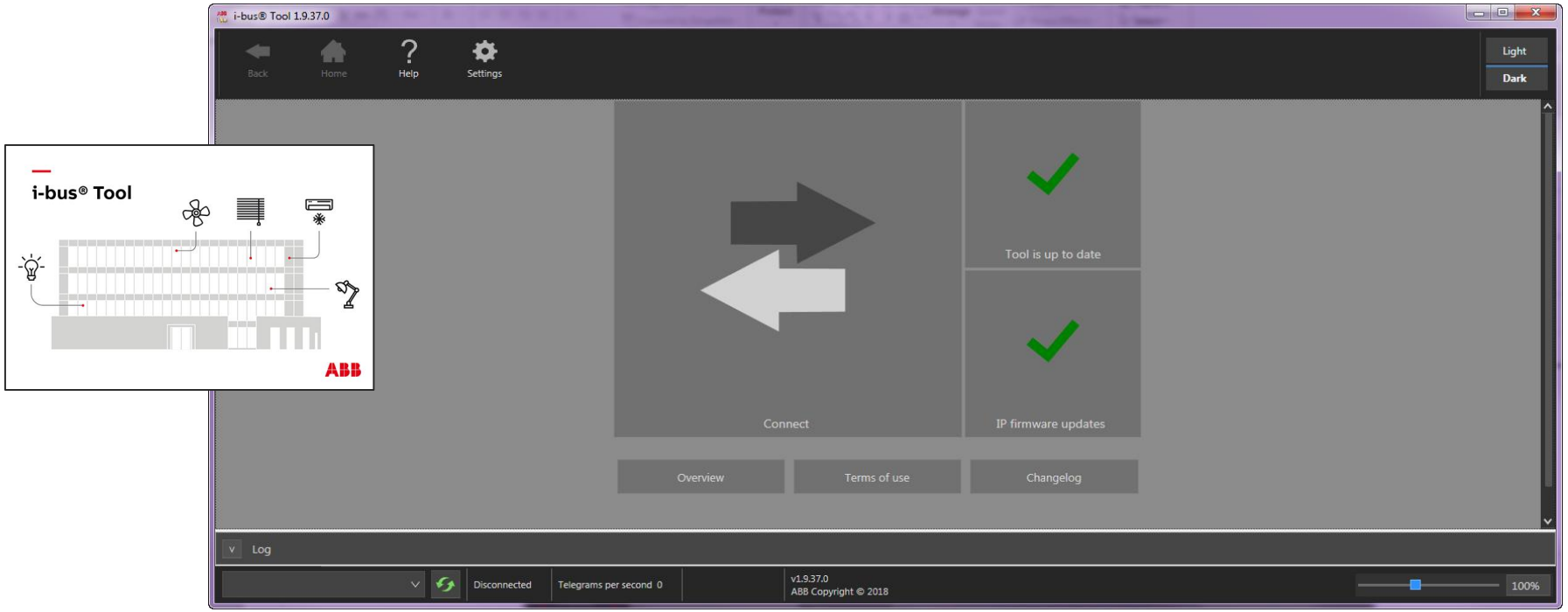
- Factory reset can be done directly on the IP Router Secure
- This does not pose a security risk because the device is no longer part of the secure system → No multicast communication to other IP Router Secure possible!!!
- Despite existing FDSK there is no access to the system (e.g. the sticker with the FDSK is still on the device)
- For commissioning and operation in KNX Secure mode, the “Backbone Key” and “Tool Key” is required!



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – i-busTool

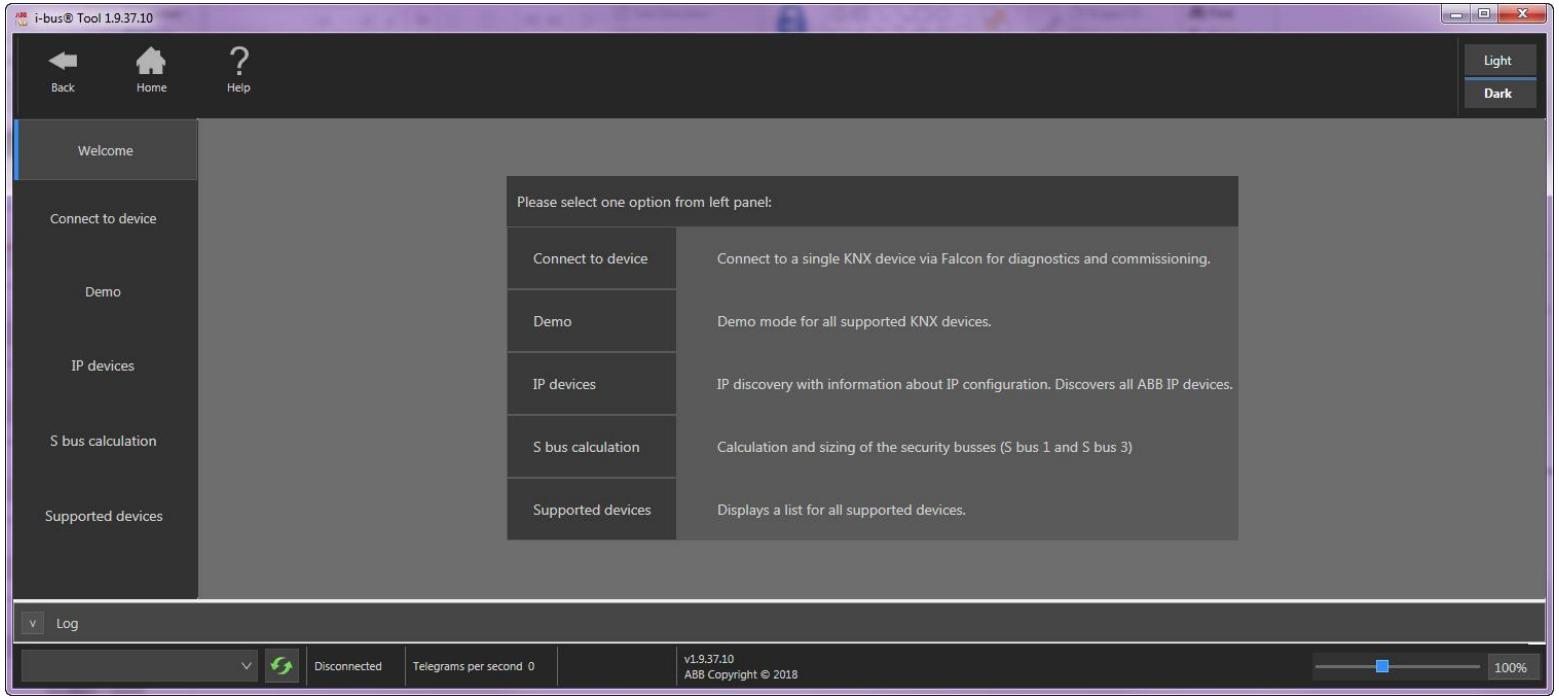
A professional diagnostics and commissioning tool



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – i-busTool

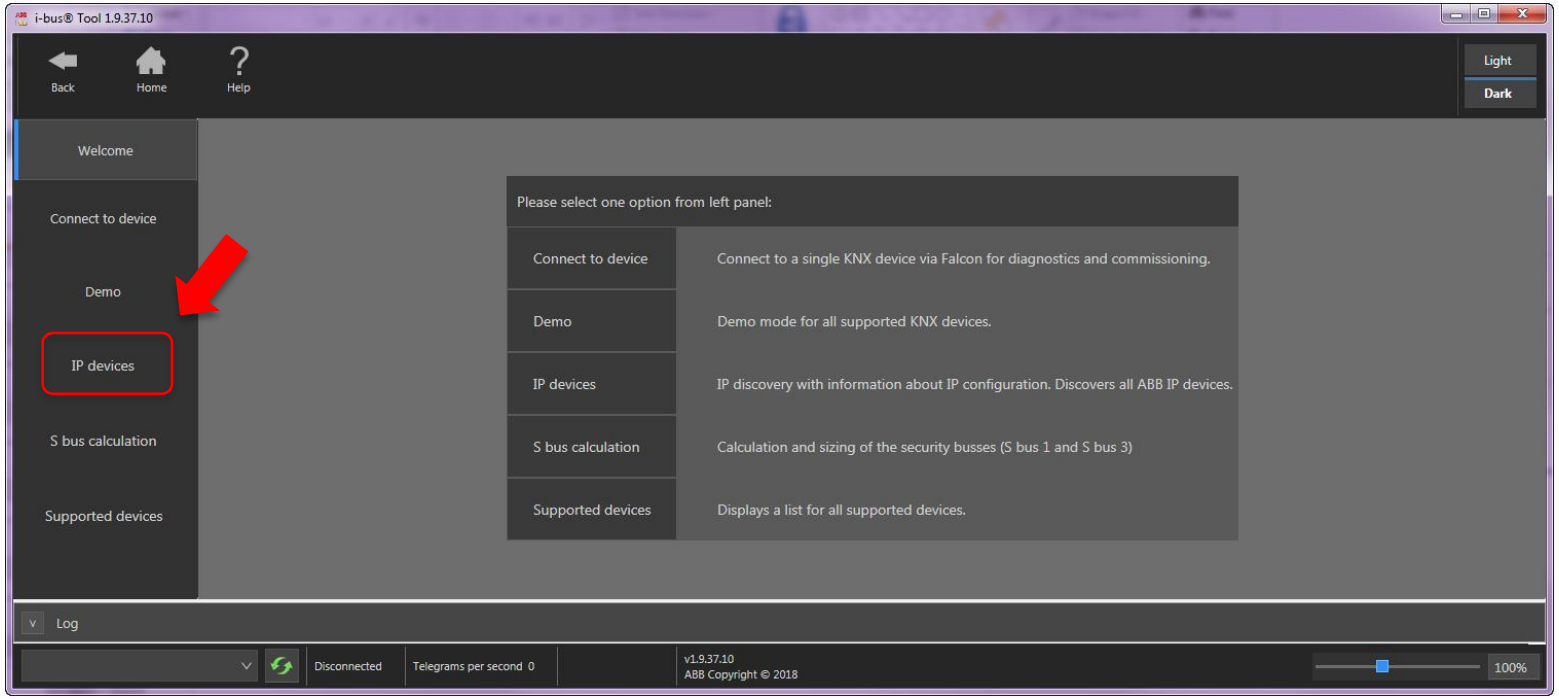
The ABB i-bus® Tool is required in order to set certain functions of the ABB IP devices and it simplifies commissioning on the IP side



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – i-busTool

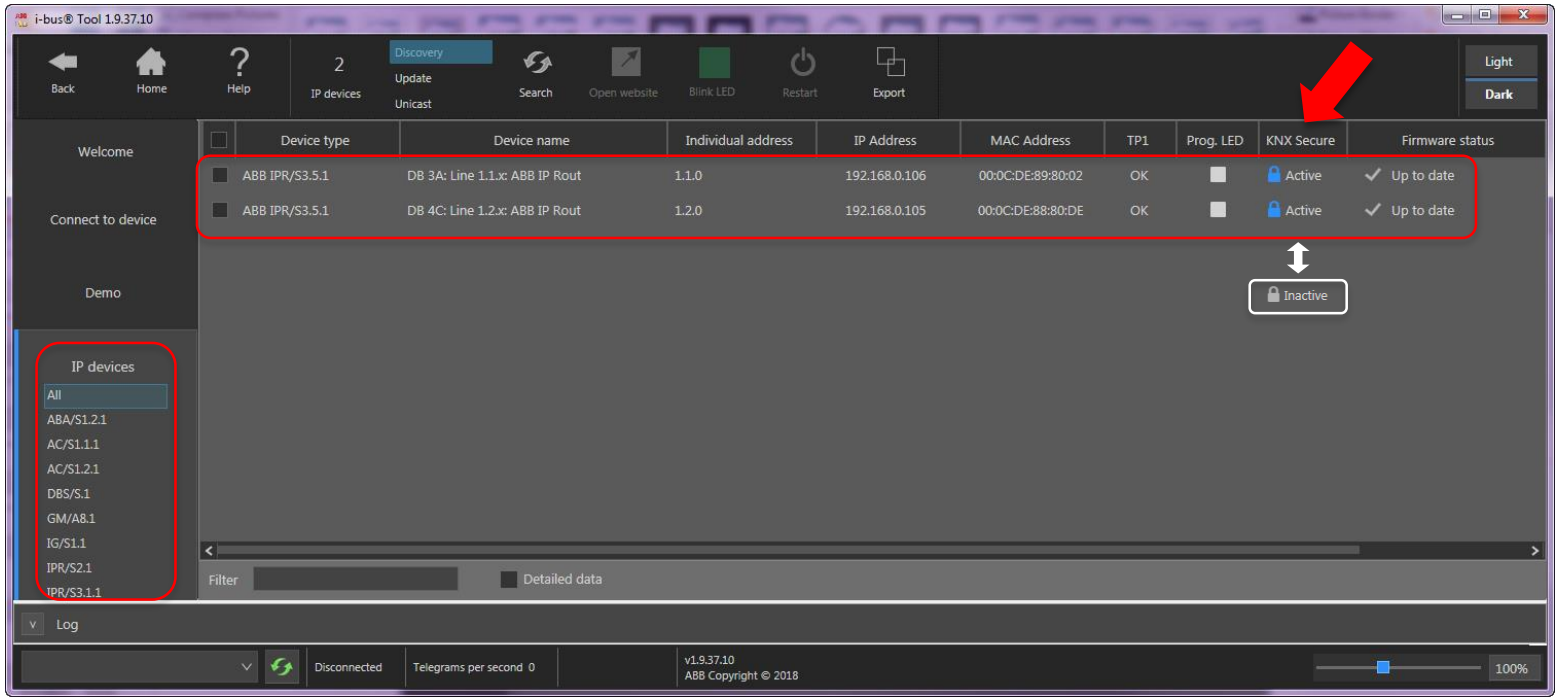
Go to the start page of the i-bus® Tool, click Connect and then click IP devices in the window that then appears



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – i-busTool

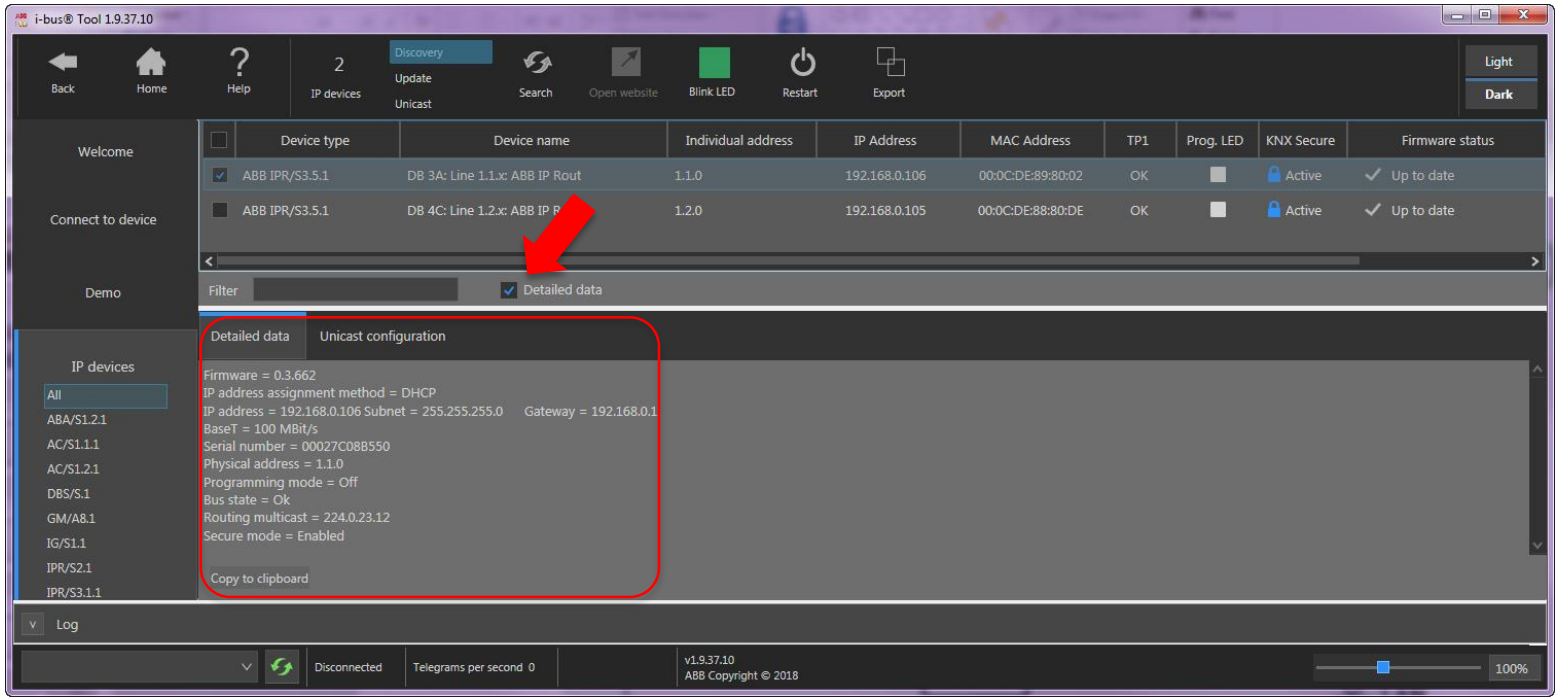
This function serves to find and display ABB IP devices in the network



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – i-busTool

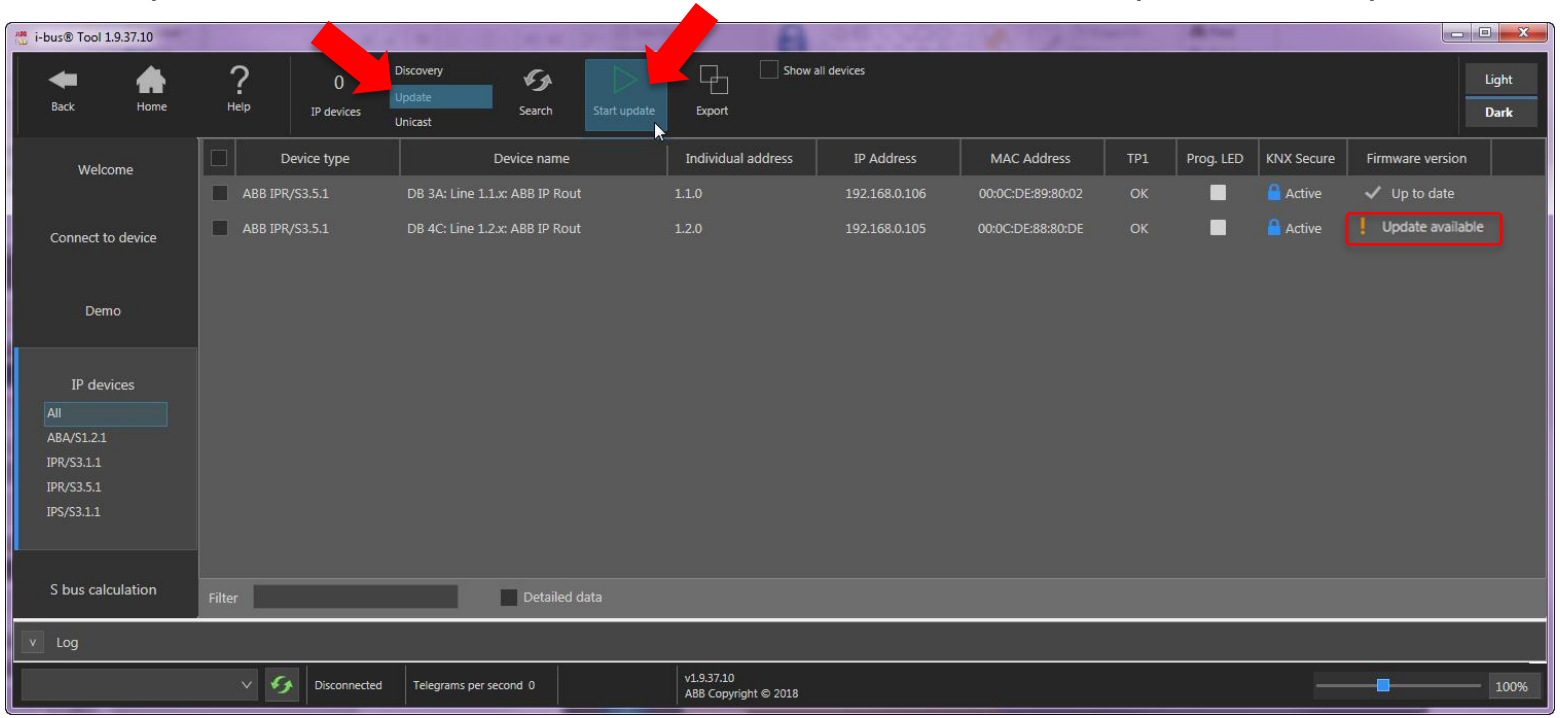
The checkbox “Detailed data” shows more details about the selected device



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – i-busTool

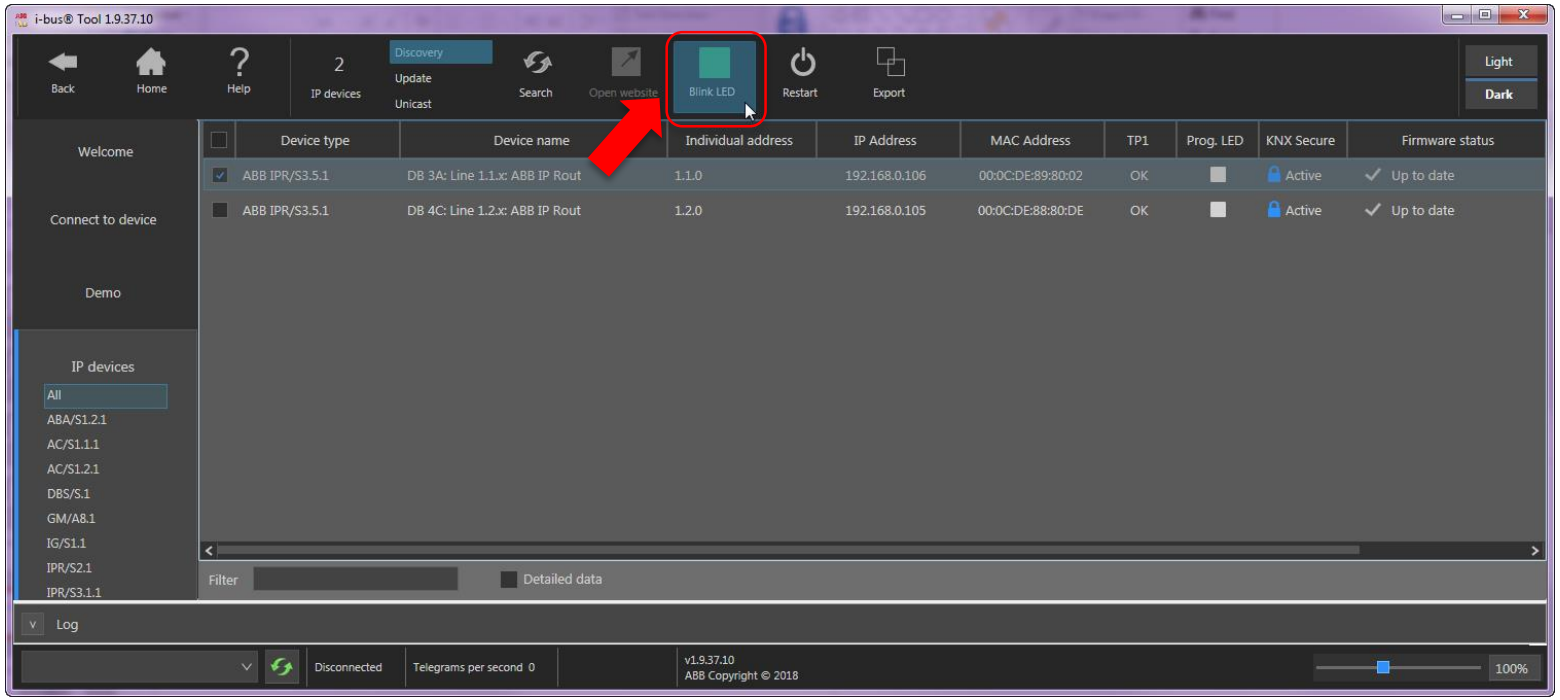
The IP Router Secure cannot be updated in KNX Secure mode. In this case, the firmware update will be possible only with the ETS app “ABB KNX Bus Update”



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – i-busTool

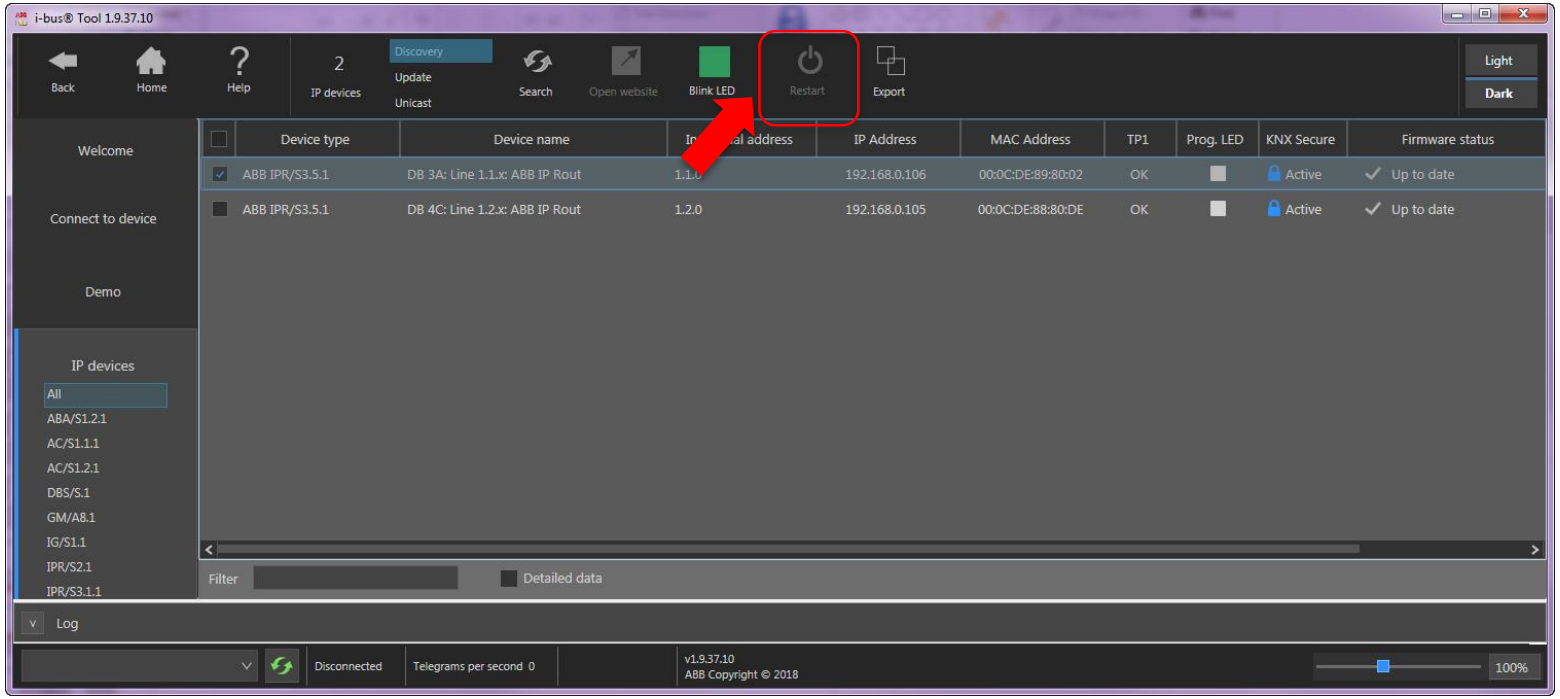
Blink LED: The LED of the selected device flashes for 5 seconds



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – i-busTool

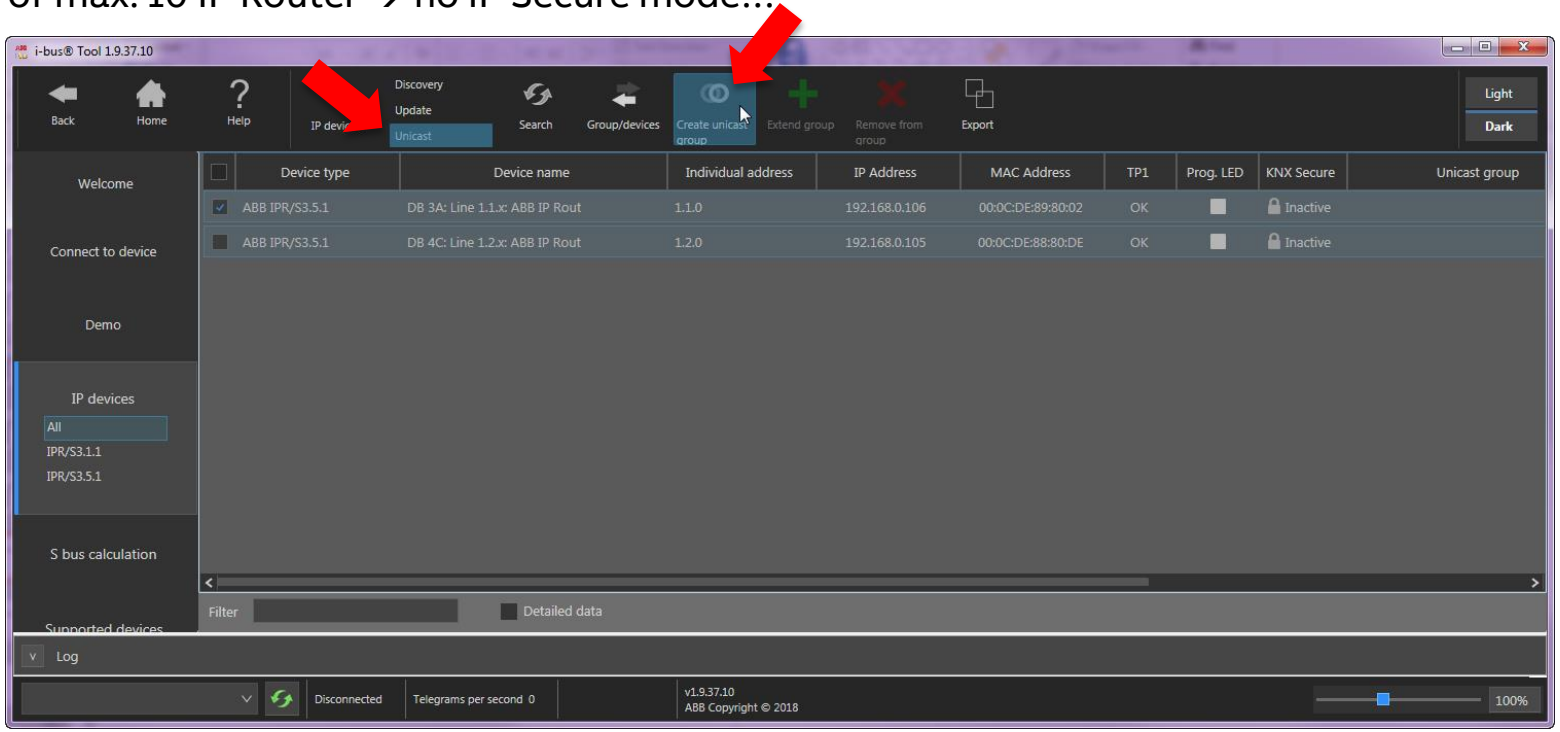
Restart device: The selected devices restart (not in IP Secure mode possible)



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

ABB IP Router Secure IPR/S 3.5.1 – i-busTool

Create “Unicast Groups” of max. 10 IP Router → no IP Secure mode!!!



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

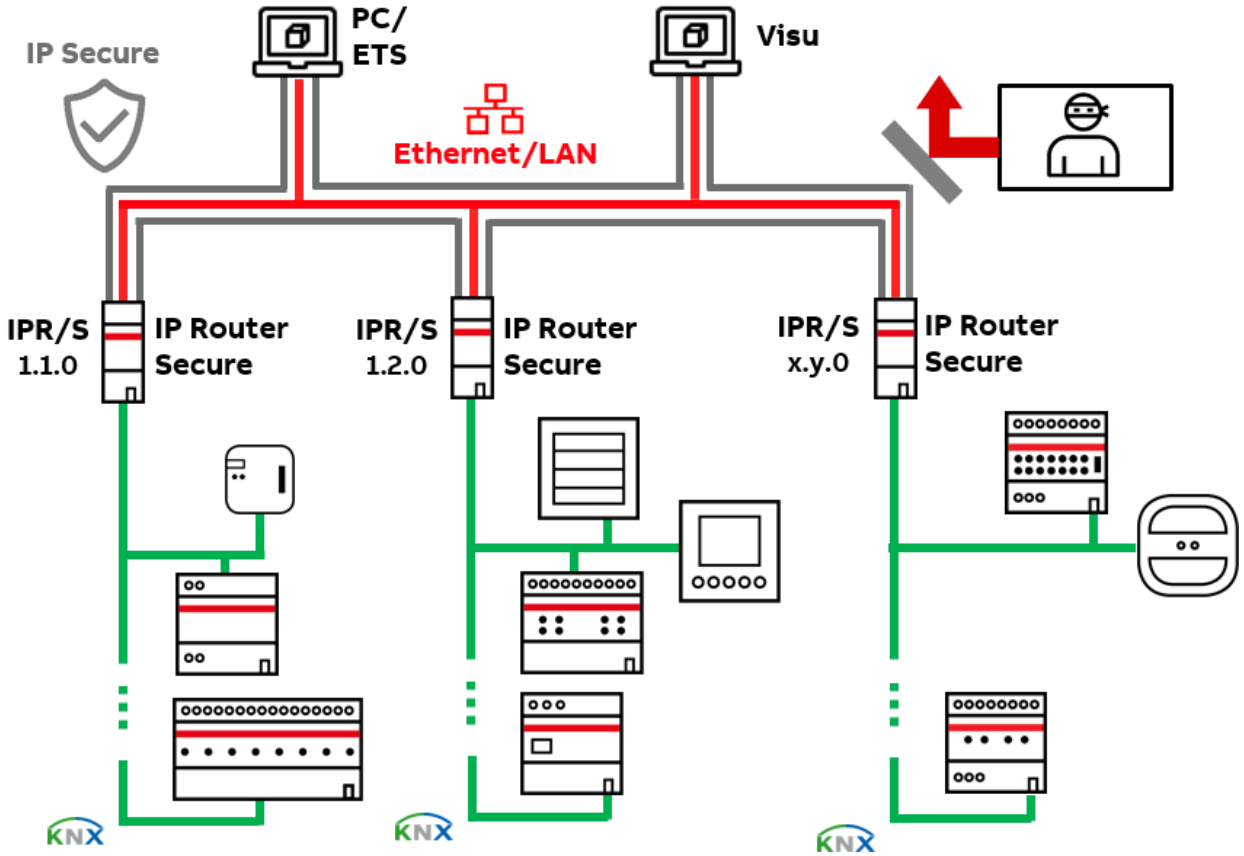
ABB IP Router Secure IPR/S 3.5.1

Summary – What is new?

- KNX IP Router Secure IPR/S 3.5.1 fulfills the KNX Secure Standard (KNXnet/IP Security)
- Communication on IP backbone, tunneling servers and commissioning from ETS are secure
- After commissioning, an IP Router Secure behaves like a standard IP Router and also has the same parameters
- All functions from standard IP Router IPR/S 3.1.1 are available
- The ETS requests a password for the project
- The ETS user only has to remember the ETS project password!
- The “Device Certificates” (FDSK) of all IP Routers Secure and other IP devices Secure must be entered
- The ETS generates and works with many keys – but there is no need to change them

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

IP Router Secure
IPR/S 3.5.1



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Training & Qualification – Database

In In this database you can find the complete online training portfolio for ABB Home and Building Automation

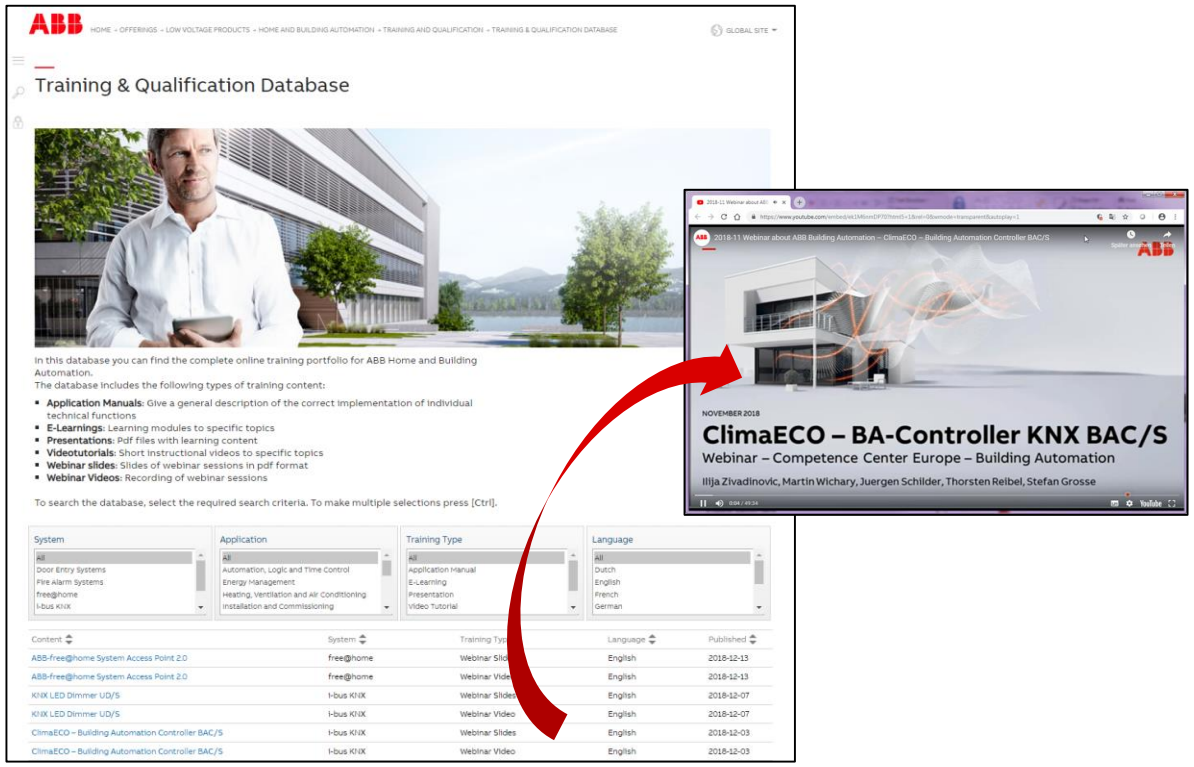
The database includes the following types of training content:

- Application Manuals
- E-Learnings
- Presentations
- Video tutorials
- Webinar slides and videos

www.abb.com/knx or https://go.abb/ba-training

→ Training and Qualification

→ Training Database



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Training & Qualification – Calendar 2019

In addition to the online modules and the traditional training programs offered by your local ABB sales team, we offer a variety of on-site trainings conducted by our specialists at different ABB training facilities

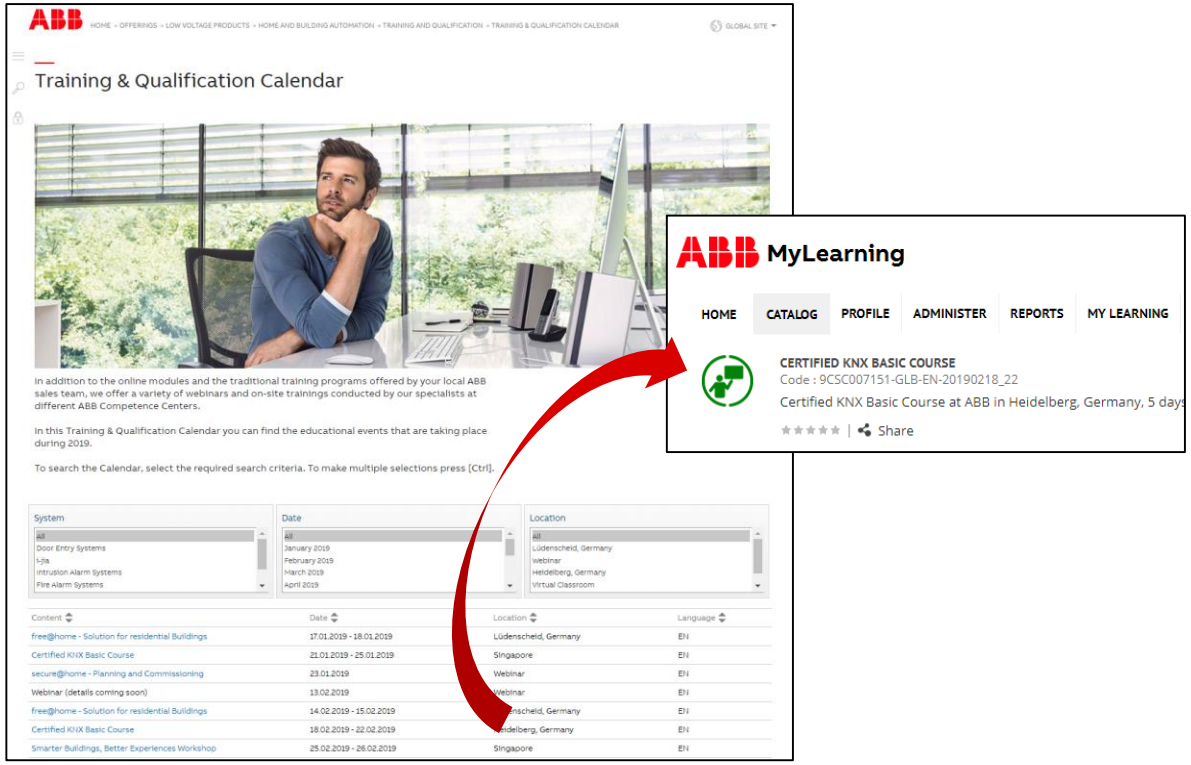
In this Training & Qualification Calendar you can find the educational events that are taking place during 2019

If you are interested in a training please click the training und you will be forwarded to register in “ABB MyLearning”

www.abb.com/knx or https://go.abb/ba-training

→ Training and Qualification

→ Training Calendar



Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

KNX Certified Training 2019

Certified KNX Courses in Heidelberg

- Advanced Course: 22nd to 26th July
- Tutor Course: 09th to 13th September
- Basic Course : 21st to 25th October
- Followed by two day application training

And many more training courses in the calendar
“International Training Dates 2019”

www.abb.com/knx or https://go.abb/ba-training

Webinar “KNX Secure and ABB IP Router Secure IPR/S 3.5.1”

Next Webinar

… the topic will be announced

Wednesday 17th April 2019

- Morning 09:00 am Europe Time (Berlin, UTC + 2h)
- Afternoon 03:00 pm Europe Time (Berlin, UTC + 2h)

Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.


ABB